United States Army

Army Knowledge Management (AKM) Guidance Memorandum - Capabilities-Based Information Technology (IT) Portfolio Governance Implementing Guidance

05 January 2006

"Our Army at War -- Relevant and Ready"

Contents (Listed by paragraph and page number)

Executive Summary

The Army Knowledge Management (AKM) Guidance Memorandum entitled Capabilities-Based Information Technology (IT) Portfolio Governance signed 20 July 2005 directs the CIO/G6, in coordination with Mission Area (MA)/Domain Leads, to issue implementing guidance. This implementing guidance is a transformational effort that defines evolving processes to ensure IT investments/capabilities:

(1) Align to support current operations and transformation;
(2) Provide measurable support to the WarFighter;
(3) Align to Mission Area/Domain portfolios; and
(4) That are interoperable, integrated and configured to support the enterprise.

The Army has a goal of identifying and reducing redundant and stove-piped IT investments by 80% by the end of Fiscal Year 2007. To achieve this goal, the Army is implementing annual Army enterprise-wide IT Portfolio Reviews of IT investments/capabilities commencing in 2nd Quarter FY06. IT investments must be managed as portfolios that are capability-based, linked to strategic goals, and linked to integrated architectures. Aligning IT investments to portfolios will allow the Army to increase efficiency/effectiveness through the elimination/consolidation of redundant or outdated capabilities, and provide increased technical performance. IT Investment portfolios will support the Army's Mission, Vision, and Goals; ensure an efficient delivery of capabilities to the Warfighter; and maximize return on investment to the enterprise.

To support IT investments/capabilities as portfolios, the Army is developing an IT Portfolio Review Process. This process will require all MA/Domain Leads to participate in Enterprise-level IT Portfolio Reviews, and at a minimum take the following actions:

(1) Maintain a baseline of all IT investment/capabilities
(a) Identify IT investments/capabilities as Core / Interim / Legacy
(b) Ensure IT investments/capabilities are registered in the Army Portfolio Management Solution - Army IT Registry (APMS-AITR) module and DoD repositories. Failure to register IT investments/capabilities in the appropriate repositories will place funding at risk
(2) Provide a plan for reducing redundant and stove-piped IT investments/capabilities by 80% by the end of Fiscal Year 2007
(3) Utilize the Army Portfolio Management Solution (APMS) as the primary portfolio management decision support tool
(4) As appropriate, verify that the portfolio complies with integration/interoperability testing and configuration management of IT investment/capabilities at the Central Technical Support Facility (CTSF)
(5) Ensure the development and utilization of MA/Domain architecture products with the Army Chief Architect.
(6) Promote Net-Centric data strategy through the use of Communities of Interest (COIs) as applicable.

Initial Army IT Portfolio Management (PfM) Reviews will be held early in the 2nd Quarter FY06 to provide an overview of each MA and their associated Domains PfM plans and processes. Regular annual PfM Reviews will commence in the 3rd Quarter FY06. After every review cycle and/or as appropriate, best practices and lessons learned will be incorporated into these processes.

This guidance applies to HQDA, its field operating agencies (FOAs), major commands (MACOMs), Program Executive Offices (PEO), and all other Army agencies or commands that define, design, implement, and integrate IT capabilities.

STEVEN W. BOUTELLE
Lieutenant General, GS
Chief Information Officer/G-6

Chapter 1
Purpose

a. This document provides guidance to implement a capabilities-based IT Portfolio Management (PfM) Process as directed by the AKM Capabilities-Based IT Portfolio Governance Memorandum (hereafter referred to as the IT Portfolio Governance Memorandum). Figure 1 outlines the Domains in the Army Mission Area/Domain Structure. The Army is institutionalizing a standard PfM process which is compliant with, and supportive of, DoD Enterprise-wide force transformation. This implementing guidance is a transformational effort that defines evolving processes to ensure IT investments/capabilities:

(1) Align to support current operations and transformation;
(2) Provide measurable support to the WarFighter;
(3) Align to Mission Area (MA)/Domain portfolios; and
(4) That are interoperable, integrated and configured to support the enterprise.

Army Mission Area/Domain Structure

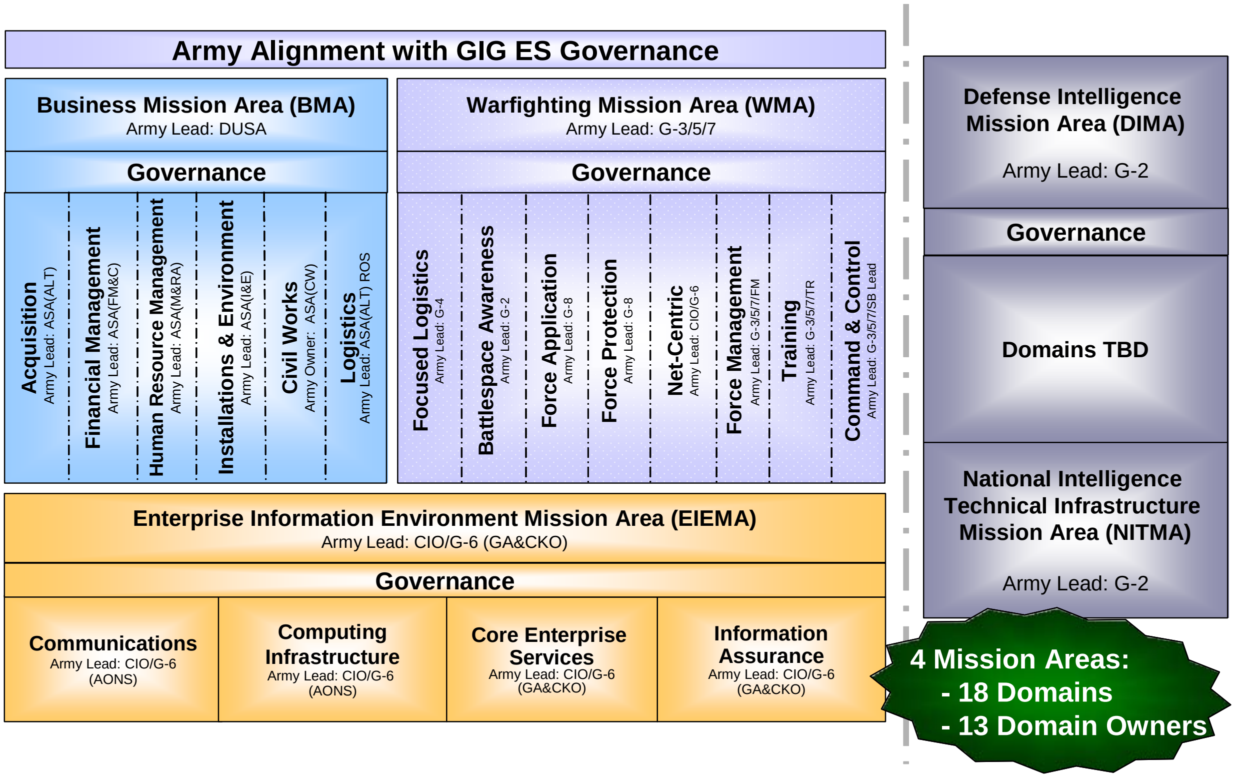


Figure 1 – Army Mission Area/Domain Structure

b. This guidance will leverage existing Army processes and procedures, while establishing a repeatable process which affords decision makers visibility of IT investments and the capabilities they provide. The PfM Process will focus on the capabilities IT investments provide to the Warfighter. This guidance will:

(1) facilitate the management and oversight of potential IT investments;

(2) encourage the use of MA/Domain architecture products to support investment decisions and facilitate the implementation of an Enterprise Architecture;

(3) support and facilitate existing decision processes, such as the Joint Capabilities Integration and Development System (JCIDS), Planning, Programming, Budgeting and Execution process (PPBE), and Defense Acquisition System (DAS), utilizing portfolios as a management tool;

(4) allow enterprise-wide participation in the management of IT investments based upon objective and measurable criteria; and

(5) facilitate JCIDS and DAS in providing input to the funding Program Evaluation Groups (PEGs) during the budget process relating to IT priorities.

Chapter 2
Background

a. IT investments/capabilities supporting the Army have grown in number, scope and complexity. As new capabilities are required and new technologies evolve, a coordinated policy and process must ensure IT investments provide the ‘right capabilities’ at the ‘right time’.

b. IT PfM is driven by the Clinger-Cohen Act (CCA) of 1996, DoD Directive 8115.01 – IT Portfolio Management, and other recent DoD and the Office of Management and Budget (OMB) direction. The PfM Process must analyze, track, and evaluate the risks and results for all IT capital investments. This process covers the life cycle of each investment and includes explicit criteria for analyzing the projected and actual costs, benefits, and risks associated for each investment.

c. DoD has established four MAs for Global Information Grid (GIG) Enterprise Services: WarFighting, Business, Enterprise Information Environment (EIE), and Defense Intelligence.

d. The IT Portfolio Governance Memorandum, co-signed on 20 July 2005 by the Secretary of the Army and the Chief of Staff Army, designates Army Leads for each MA and Domain. This designation of Army Leads aligned with the DoD construct establishes reporting authorities and responsibilities consistent with current laws, policies and regulations.

Chapter 3
Applicability & Scope

3-1. Applicability

This PfM guidance applies to all components of the Army.

3-2. Scope

a. This document provides processes, procedures, guidance, and responsibilities for the MAs and their Domains in the management of IT investments as portfolios. The PfM Process will ensure that IT investments are capability-based and linked to strategic goals. They must promote and support interoperability, Information Assurance, Joint and Expeditionary operations, and the modular force structure. IT investment decisions will include consideration of:

(1) appropriate risk tolerance levels,

(2) increased efficiencies

(3) elimination/consolidation of redundant or stove-pipe IT investments/capabilities

(4) appropriate architecture products.

b. IT PfM governance includes all Army IT investments that are connected to the GIG. This includes all MA and Domain systems that exchange information through the Defense Information Systems Network and the LandWarNet, which enables improvements in collaboration, analysis, decision making, situational awareness, and integration; as well as providing a more capable and reliable network. Effective IT infrastructure, information assurance, architecture, and associated investment oversight are essential to achieving integrated end-to-end (E2E) Enterprise Solutions for meeting capability requirements.

c. It is imperative that the Army develop a formal, structured, repeatable IT PfM Process for the enterprise. To facilitate this effort, this document outlines guidance for implementing directives associated with the IT Portfolio Governance Memorandum. It also articulates the roles, responsibilities, processes, tools, and information needed to determine and continuously adjust the optimum set of Army Enterprise IT investments needed to support all four MAs.

d. For the Army Enterprise IT PfM Process to be effective, it must be integrated with a solid foundation that includes an Enterprise Architecture (EA) development and validation process. The Army's PfM Process will capitalize upon the Army Enterprise Architecture (AEA) as well as other existing architectures, such as the Business Enterprise Architecture (BEA) within the Business Mission Area. The Army CIO/G-6 serves as the integrating office for all architecture requirements, products, and solutions.

e. To support MAs/Domains PfM processes, the Army has multiple responsibilities that the scope of this document covers:

(1) Implement the Army Enterprise PfM Process;

(2) Perform IT portfolio reviews and recommend initiative funding as part of the PfM process;

(3) Develop MA/Domain Architectures in accordance with AEA guidelines;

(4) Enforce compliance with transformation plans; and

(5) Guide PfM execution activities.

Chapter 4
Army IT Portfolio Management (PfM) Process

4-1. The Army IT PfM Process

a. The PfM methodology complies with the OMB's A-130 policy guidance and DoDD 8115.01 which require agencies to determine the following, before committing resources to any existing or new capital asset:

(1) whether the asset supports core mission functions,

(2) whether any other government or private entity can provide the service better, and

(3) whether agency business processes have first been reengineered to provide optimal performance at the lowest cost.

b. Figure 2 depicts the Army's IT PfM Process (as further defined in Appendix A) as implemented by this document, which will include visibility of all MA and Domain IT capabilities, initiatives, requirements, funding, and systems necessary to support joint interoperability. It incorporates current Department of the Army, Department of Defense (DoD) direction, guidance per the Clinger-Cohen Act (CCA) of 1996 and relevant National Defense Authorization Act (NDAA) direction. Six core continuous PfM activities/phases are used to manage the portfolios and are an integral part of the PfM Process. Details on each step under the six core PfM activities/phases can be found in Appendix A.

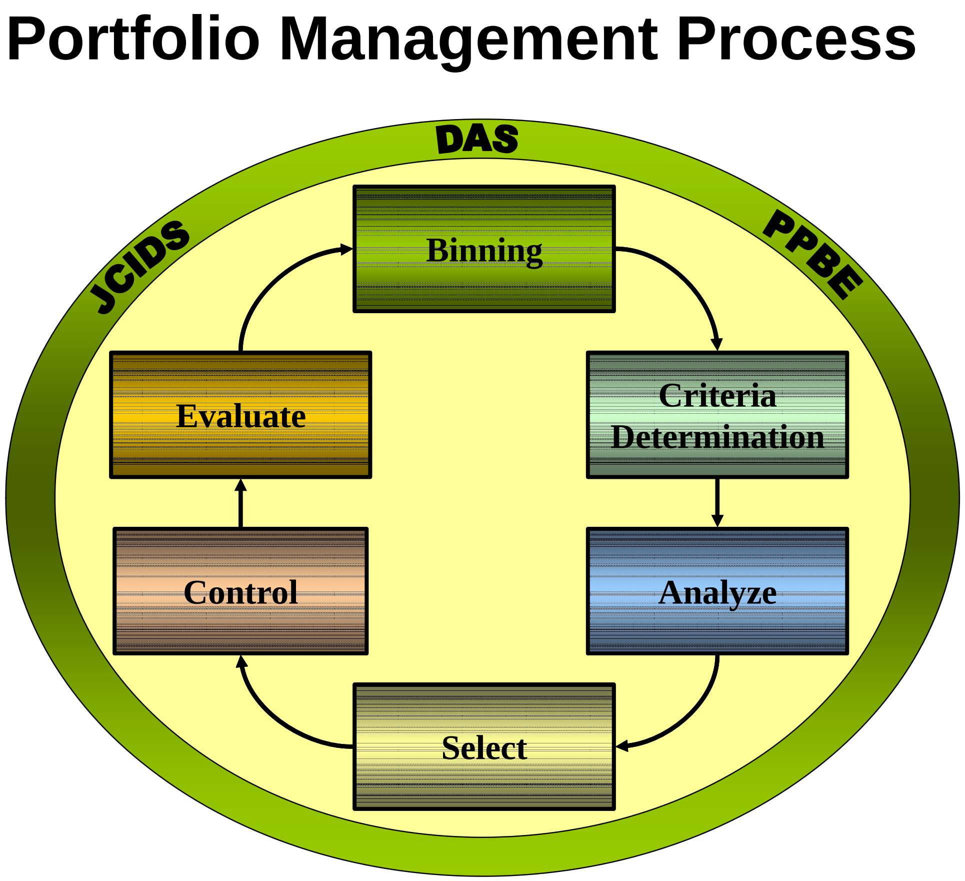


Figure 2 – Portfolio Management Process

(1) ***Binning*** is the activity that assigns capabilities/investments to the governing Army IT MA/Domains. IT Domain binning will be synchronized with other DoD/Army processes.

(2) ***Criteria Determination*** is the activity that defines portfolio goals, assessment metrics, and risk assessment criteria used to analyze Army IT investments. Criteria determination is typically covered as part of the analyze activity; however it is addressed separately here to highlight its importance.

(3) ***Analyze*** is the activity that builds on requirements for analysis of existing IT capabilities and alternatives. This activity links portfolio objectives to Enterprise vision, mission, goals, objectives, and priorities; develops quantifiable outcome-based performance measures; identifies capability gaps, opportunities, and redundancies; identifies risks; provides for continuous process improvement; and determines strategic direction of selected MA.

(4) ***Select*** is the activity that identifies and selects the best mix of IT investments to strengthen and achieve capability goals, mission outcomes and objectives for the portfolio and demonstrates the impact of alternative IT investment strategies and funding levels.

(5) ***Control*** is the activity that ensures a portfolio and individual IT investments within the portfolio are managed and monitored using established quantifiable outcome-based performance measures; provide intended capabilities; and are acquired within cost, schedule, and performance

baselines. Portfolios are monitored and evaluated against portfolio performance measures to determine whether to recommend continuation, modification, or termination of individual investments within the portfolio.

(6) ***Evaluate*** is the activity that measures actual contributions of the portfolio and its identified capabilities and IT investments against established outcome-based performance measures to determine improved capability as well as to support adjustments to the mix of portfolio investments, as necessary.

c. The IT PfM Process will identify capability gaps and redundancies, which are then fed to the JCIDS, DoD 5000, and/or PPBE processes for appropriate action.

d. The Army will support the PfM Process with tools provided by the Army Portfolio Management Solution (APMS) consisting of the Army IT Registry (APMS-AITR) module, Domain Certification (APMS-DC) module, Capital Planning and Investment Management (APMS-CPIM) module, and Capital Planning and Investment Control (APMS-CPIC) module. APMS empowers users at all levels within the enterprise and standardizes common data elements used in IT PfM. APMS standardizes reporting procedures for IT investments, allowing MA/Domain Leads to manage their portfolios and align capabilities with MA and Domain investment strategies.

4-2. Army IT PfM Review Process

a. The following activities are required to perform Enterprise Level Portfolio Reviews. (See Figure 3)

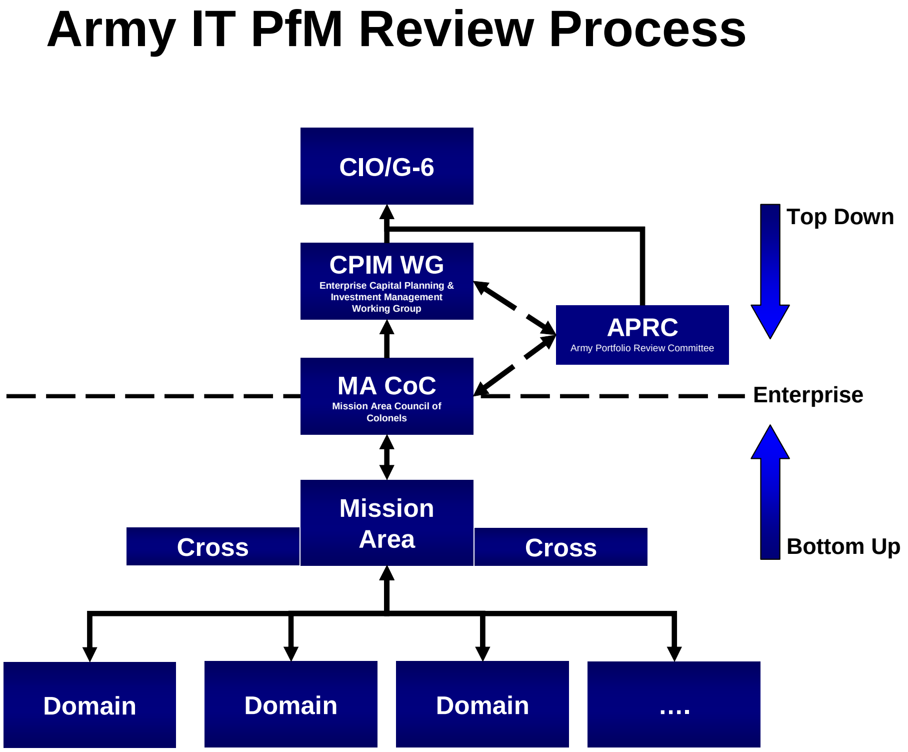

Army IT PfM Review Process
CIO/G-6
Top Down
CPIM WG
Enterprise Capital Planning & Investment Management Working Group
APRC
Army Portfolio Review Committee
MA CoC
Mission Area Council of Colonels
Enterprise
Cross
Mission Area
Cross
Bottom Up
Domain
Domain
Domain
....

Figure 3 – Army IT PfM Review Process

(1) MAs/Domains create internal governance forums, at their level, to review and assess their respective IT portfolios and conduct internal portfolio reviews.

(2) MAs/Domains participate in annual preliminary Enterprise Level MA/Domain Reviews conducted by the Mission Area Council of Colonels (MA CoC).

(3) Using the output from these reviews, the Enterprise CPIM Working Group (CPIM WG) conducts review and analysis of MA IT capabilities and requirements to gain cross MA efficiencies and to prioritize the Army IT investment strategy. The CPIM Process validates MA strategies and prepares a consolidated IT Investment Strategy for use in the POM process, providing both to the appropriate PPBE Review Board.

(4) The Army Portfolio Review Committee (APRC) will meet as required, conduct the final Enterprise Level MA/Domain Portfolio Reviews, resolve cross-MA issues, and forward Portfolio Review results/recommendations to the CIO/G-6.

b. **Mission Area Council of Colonels (MA CoC)**

(1) The MA CoC (see Figure 4) is quad-chaired by COL/GS-15 level representation from G-3/5/7, Assistant Secretary of the Army (Financial Management and Comptroller) (ASA(FM&C)), G-8 and the Chief Information Officer/G-6 (CIO/G-6). The MA CoC will have representation from the Business, Warfighting, EIE, and Defense Intelligence MAs, Office of General Counsel (OGC), the Army Audit Agency (AAA), Special Assistant Secretary of the Army - Business Transformation (SASA-BT), Army Staff (ARSTAFF), Major Commands (MACOMs), Assistant Secretary of the Army (Acquisition, Logistics, & Technology) (ASA(AL&T)), and the Domains as appropriate.

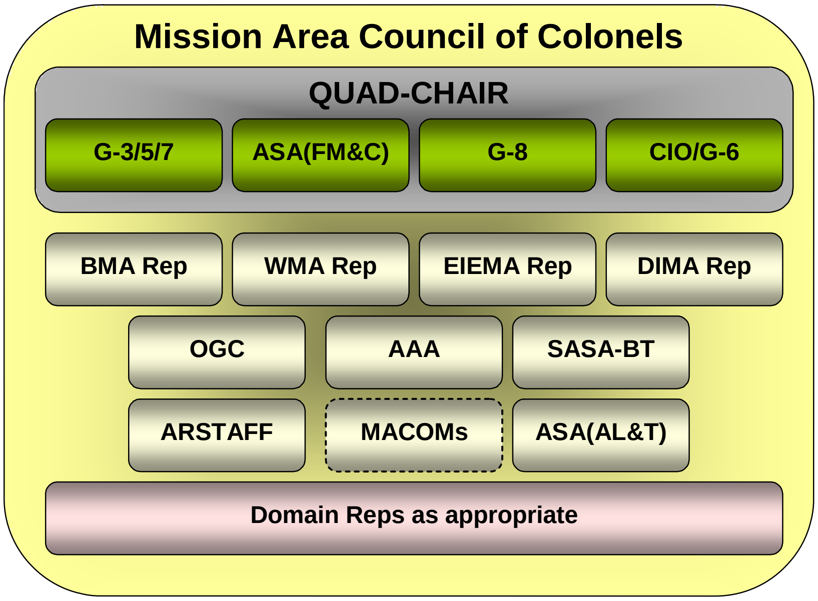


Figure 4 – Mission Area Council of Colonels

(2) The MA CoC will review, analyze, and validate the MA/Domain IT portfolios capabilities against Army strategies and tactical requirements.

(3) The MA CoC will review and analyze the products from the preliminary MA/Domain Portfolio Reviews, verifying identified gaps and overlaps, validating the MA transition planning and cross MA efficiencies by:

(a) Conducting MA/system portfolio reviews in alignment with IT requirements and capabilities

(b) Validating internal MA IT investments (consolidations/eliminations) IAW MA Strategy.

(c) Validating MA compliance and certification requirements.

(d) Validating MA investments/capabilities and strategy, influencing and supporting the Enterprise CPIM WG/PPBE Reviews.

c. **Enterprise Capital Planning & Investment Management Working Group (CPIM WG)**

(1) The CPIM WG captures the products of the MA CoC to review the results for the Enterprise/Cross-MA level to identify potential redundancies/inefficiencies and best practices for application across the Enterprise. The CPIM WG traces each potential IT investment/capability to the actual or proposed funding source (depending upon current or future investment). An analysis of how each IT investment/capability contributes to Army strategic direction and priorities allowing prioritization of the IT investments by Management Decision Evaluation Package (MDEP) within the funding PEG, in support of the PPBE process and Army Enterprise Strategy.

(2) The CPIM WG (see Figure 3) will:

(a) Verify that MA/Domain/Functional requirements and IT capabilities have been identified and documented against Army Strategy

(b) Analyze IT funding requirements for cross-MA efficiencies

(c) Evaluate each proposed IT investment against common evaluative criteria to determine contribution to achievement of Army priorities

(d) Prioritize IT investments in support of the PPBE process based upon Army strategic direction and the CIO/G6 enterprise objectives in support of the Army Enterprise.

(3) In accordance with the CPIM Charter, the CPIM WG is a collaborative effort comprised of the Army's multi-functional community of C4/IT stakeholders, who collectively determine the Army's "best value" investment solutions to meet the required capabilities. To accomplish this, the CIO/G-6 depends heavily upon subject matter experts (SMEs). Each MA and Domain will have a CPIM WG representative.

(4) Common evaluative criteria are used to subjectively evaluate proposed IT investments. This subjective evaluation, supported by APMS, provides an initial investment prioritization, which is then reviewed for evolving direction and priorities.

(5) The CPIM developed Army IT Investment strategy is reviewed by the Army CIO/G6 in accordance with Clinger-Cohen responsibilities, and once codified, furnished to the PEGs for their use in the PPBE process.

(6) To this end the CPIM program provides critical IT investment recommendations to integrate with the JCIDS, PPBE, and DAS.

d. **Army Portfolio Review Committee (APRC)**

(1) The APRC Quad-Chair (see Figure 5) is composed of the Deputy Assistant Chief of Staff G-3/5/7, the Deputy Assistant Secretary of the Army (Financial Management and Comptroller) (ASA(FM&C)), the Deputy Assistant Chief of Staff G-8 and the Deputy Chief Information Officer/G-6 (CIO/G-6). The APRC PfM Review meetings will have potential GO/SES level attendees with representation from Assistant Secretary of the Army (Acquisition, Logistics, & Technology) (ASA(AL&T)), Office of General Counsel (OGC), the Army Audit Agency (AAA), Business, Warfighting, EIE, and Defense Intelligence MAs, Assistant Secretary of the Army (Financial Management and Comptroller) (ASA(FM&C)), G-8, Special Assistant Secretary of the Army - Business Transformation (SASA-BT), G-4, and the other Domains within the same MA under review.

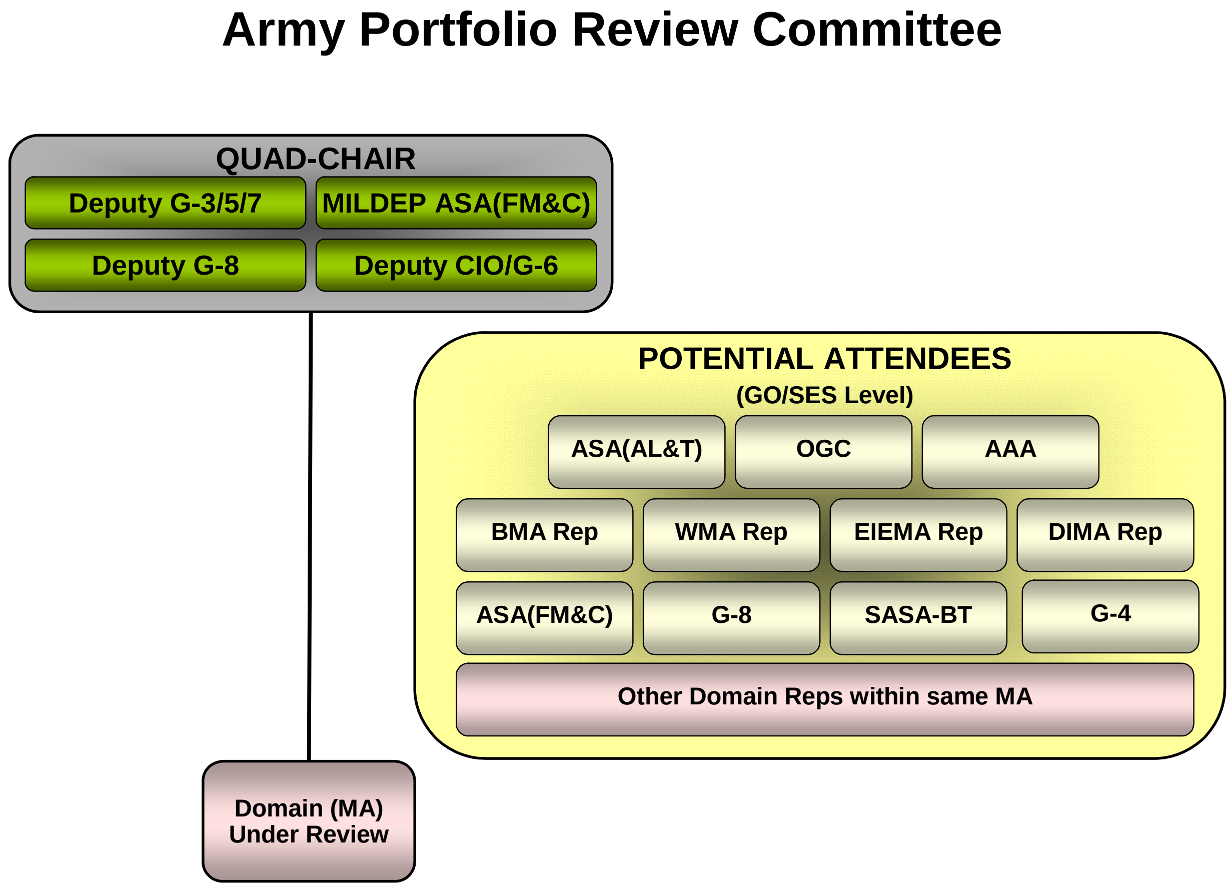


Figure 5 – Army IT PfM Review Process

e. **Army's PfM Reviews**

(1) Starting in FY2006 the APRC will conduct annual Enterprise Level MA/Domain PfM Reviews, utilizing the APMS - Portfolio Management Decision Support Tool. The IT Portfolio Reviews will include the following MAs:

(a) Enterprise Information Environment Mission Area (EIEMA)

(b) Business Mission Area (BMA)

(c) Warfighting Mission Area (WMA)

(d) Defense Intelligence Mission Area (DIMA)

(2) For the reviews, the MAs will provide the following information at a minimum but not limited to:

(a) Provide Mission Area Vision, Capabilities, and Governance Processes

(b) Provide status of systems by Domain

(i) Identify IT investments/capabilities as Core / Interim / Legacy

(ii) Ensure IT investments/capabilities are registered in the Army and DoD repositories. Failure to register IT investments/capabilities in the appropriate repositories will place funding at risk

(c) Provide a plan for reducing redundant and stove-piped IT investments/capabilities by 80% by the end of Fiscal Year 2007

(d) Utilize the Army Portfolio Management Solution (APMS) as the primary portfolio management decision support tool

(e) As appropriate, verify that the portfolio complies with integration/interoperability testing and configuration management of IT investment/capabilities at the Central Technical Support Facility (CTSF)

(f) Ensure the development and utilization of MA/Domain architecture products with the Army Chief Architect.

(g) Promote DoD and Army guidance for Net-Centric data strategy (DoDD 8320.2 – Data Sharing in a Net-Centric Department of Defense, AR25-1). As required, participate in or establish Communities of Interest (COIs) to develop and implement DoD and Army data strategies.

(3) To the maximum extent possible, MA/Domain Portfolio Reviews will utilize APMS. More detailed guidance on review format is provided in Appendix B.

f. **CIO/G-6** - The CIO/G-6 receives and reviews products from the both CPIM WG and APRC and complies with Clinger-Cohen responsibilities. The CIO/G-6 provides a prioritized listing of all IT investments, by MDEP to the PEGs. These products will be used by the PEGs for budget deliberations within the PBBE process. The results of the IT PfM reviews will also provide information that can be used for updating Army strategic documents including: The Army Plan, the Army Program Guidance Memorandum, and the Army Campaign Plan.

Chapter 5
Responsibilities

5-1. Governance

This section defines the responsibilities required to execute Army PfM.

***a.* Mission Area Leads (Specific)**

(1) The DUSA, or his designated representative, as the Army's BMA Lead will ensure generating force efforts are traceable to, and fully support, the required capabilities for the WMA, DIMA, and EIEMA. Additionally, this MA Lead will ensure that a single integrated Architecture for the BMA efforts exists to support the Business Enterprise Architecture (BEA).

(2) The Chief Information Officer/G-6, as the Army's EIEMA Lead, will ensure EIE efforts are traceable to, and fully enable, the required capabilities for the WMA, DIMA and BMA. In addition, this MA Lead will provide Domain leadership for the Net-Centric Domain.

(3) The Deputy Chief of Staff, G-3/5/7, as the Army's WMA Lead, will approve, prioritize, and synchronize all GIG capabilities, experimentation, concepts, and architecture development efforts for the WMA.

(4) The Deputy Chief of Staff, G-2, as the Army's DIMA and National Intelligence Technology Infrastructure Mission Area (NITMA) Lead, will ensure that intelligence efforts are traceable to, and fully support, the required capabilities for the WMA and EIEMA. Additionally, this MA Lead will ensure that a single integrated architecture for the National Geospatial-Intelligence Agency efforts exists to support the Battlespace Awareness Domain of the WMA.

***b.* Mission Area Leads (General)**

(1) Establish MA IT PfM direction and plans for MA GIG capabilities, Enterprise solutions, experimentation, concepts, and operational architecture development efforts.

(2) Ensure the development and utilization of MA/Domain architecture products with the Army Chief Architect.

(3) Identify Domain Leads and ensure linkages to existing DoD Domains, in coordination with their DoD MA and Domain Leads and their Army counterparts.

(4) Provide an MA IT PfM Plan that considers end-to-end (E2E) processes IAW DoD and Army Guidance.

(5) Establish key metrics, timelines, and milestones to track IT Transformation.

(6) Require internal MA portfolio reviews to be conducted for each subordinate Domain

(7) Verify identified funding through appropriate channels.

(8) In coordination with CIO/G-6, develop outcome-oriented performance measures that are aligned with strategic guidance from the President, SECDEF, SA, and MA strategic goals and objectives.

(9) Include the G-3/5/7 and the G-8 in portfolio reviews to ensure IT capabilities/initiatives prioritization and funding are addressed.

(10) Provide an outline of their MA unique PfM plans and processes in their respective appendix of this guidance.

***c.* Domain Leads**

(1) IAW MA guidance, establish Domain IT PfM plans and processes.

(2) Establish and validate Domain level IT investment baseline against Domain designated portfolios.

(3) Support architecture development in accordance with Appendix D and any other applicable guidance.

(4) Utilize the APMS – IT portfolio management decision support tool for conducting Domain IT PfM activities and determining within Domains where capability redundancies/gaps exist and where integration of products and services might better support warfighter needs. The APMS will be used to conduct regularly scheduled PfM Reviews.

(a) Develop and maintain a Domain IT Portfolio of systems by capability.

(b) Identify and prioritize investments to satisfy Domain IT capabilities.

(5) Recommend opportunities for cross Domain integration to continually improve delivery of IT-based capabilities in support of warfighter needs.

(6) Utilize existing Army processes (JCIDS, PPBE, and DAS) to prioritize, synchronize and fund opportunities identified by PfM processes.

(7) As required, review a business case analysis for those planned IT expenditures that have enhancements of more than $1M across the Future Year Defense Program (FYDP).

(8) Evaluate all Domain and sub Domain proposed IT Portfolio investments based on:

(a) Capability provided

(b) Architecture products

(c) Criticality to Mission

(d) Interoperability

(e) Risk

(f) Strategic Alignment

(g) Performance Metrics

(h) Program resources/costs

(9) Ensure all Domain IT investment reviews focus on capabilities, and include the full life cycle costs of IT expenditures.

(10) Participate in enterprise governance forums, as required, to identify opportunities for commonality in PfM techniques, and provide solutions that are in the best interest of the Enterprise.

(11) Establish and utilize outcome-oriented IT performance measures that are aligned with strategic guidance and the MA balanced scorecard in the Strategic Readiness System (SRS). Progress will be reviewed and reported through the governance structure.

(12) Establish, in coordination with the MA, key metrics, timelines and milestones to track IT Transformation.

(13) Coordinate, as required, with the G-3/5/7 and the G-8 to ensure issues of portfolio/system prioritization and funding are addressed during portfolio reviews.

(14) Develop IT investment strategies that are capabilities focused, and manage Domain IT investments.

(15) Promote DoD and Army guidance for Net-Centric data strategy (DoDD 8320.2 – Data Sharing in a Net-Centric Department of Defense, AR25-1). As required, participate in or establish Communities of Interest (COIs) to develop and implement DoD and Army data strategies.

***d.* Army Portfolio Review Committee (APRC)**

(1) Conduct Enterprise Level Domain IT PfM Reviews

(2) Adjudicate cross-MA issues.

(3) Validate internal Domain IT investments

(4) Validate Domain compliance and certification requirements funding to DoD

(5) Validate IT investments/capabilities and strategy influencing and supporting Enterprise CPIM Working Group/PPBE Reviews

(6) Provide recommendations to the CPIM WG on IT investments

(7) Approve MA Portfolio Binning lists

(8) Review and approve MA/Domain metrics.

***e.* Capital Planning & Investment Management Working Group (CPIM WG)**

(1) Verify that MA/Domain/Functional requirements and IT capabilities have been identified and documented against Army Strategy

(2) Analyze IT funding requirements for cross-MA efficiencies

(3) Evaluate each proposed IT investment against common evaluative criteria to determine contribution to achievement of Army priorities

(4) Prioritize IT investments in support of the PPBE process based upon Army strategic direction and the CIO/G6 enterprise objectives in support of the Army Enterprise.

***f.* Deputy Under Secretary of the Army Operations Research (DUSA(OR))**

(1) Assist, as required, the MA/Domains in the development of their metrics.

(2) Assist the MA/Domains in their Analyze and Select Phase processes.

(3) Integrate information requirements into APMS to support IT investment decision processes.

***g.* ASA(AL&T)**

(1) Ensure Program Executive Officers (PEOs)/Program Managers (PMs) input data into the APMS to support MA/Domains IAW this document.

(2) Ensure PEOs/PMs participation in the MA/Domain IT PfM processes.

(3) Provide System Architectures in support of Army IT PfM.

***h.* G3/5/7**

(1) Serve as the ARSTAFF focal point for organization, integration, decision-making, and execution of the spectrum of activities encompassing requirements definition, force development, force integration, force structuring, combat developments, training developments, resourcing, and prioritization.

(2) Serve as the focal point for prioritization, integration, and synchronization of capabilities and requirements made both on the ARSTAFF and externally.

(3) Serve as the overall integrator of Army transformation.

(4) Serve as the Chief Architect of the Army in support of PfM.

i. **G8**

(1) Manage the programming phase of the Army PPBE to facilitate the development of the Army program and the transition to an Army Budget Estimate Submission (BES).

(2) Responsible for transitioning approved Army requirements from the planning to the programming phase.

(3) Responsible as principal advisor to the CSA on Joint materiel requirements, doctrine, training, leader development, organizations, and materiel - personnel and facilities (DTLOM-PF) integration, and materiel program execution over their life cycles.

(4) Assist Domains with their PfM processes (Directorate of Materiel (DOM)).

(5) Provide guidance on appropriate documentation required to support PPBE activities.

j. **CIO/G-6**

(1) Serve as the APRC and Senior Review Group (SRG) Executive Secretary.

(2) Provide IT PfM policy guidance and oversee implementation of MA / Domain’s IT portfolios to ensure they are aligned with Army Enterprise Solutions.

(3) Serve as the single Army interface with the Office of the Secretary of Defense (OSD) Transformation Support Office (TSO), OSD Domain Leads, OSD MA Leads, Army MA Leads, Army Domain Leads, and the Army Functional Domain Leads for all IT related data calls and other IT MA requirements.

(4) Serve as the Pre-Certification Authority (PCA) for OSD Certification Reviews (for example, BMMP Certifications).

(5) Support Net-Centric Data Strategy.

(6) Serve as the Army Lead/coordination authority for all GIG ES IT related actions.

(7) Review and revise the current process for maximizing the value, and assessing and managing the risks of Army IT investments across the Enterprise, ensuring consistency with evolving DoD policy.

(8) Review and revise the Army IT PfM Process IAW evolving DoD guidance/policy, fully incorporating the DoD MA/Domain construct and the necessary program review requirements. Ensure PfM processes are incorporated into, and integrated with, each of the principal decision support systems: JCIDS, PPBE, and the DAS.

(9) Establish enterprise level performance measures as an integral component of the transformation strategy, aligned with mission, vision, goals and objectives. The CIO/G-6 will provide core criteria and metrics to track and measure capabilities provided by IT investments against the established performance criteria embedded in the SRS.

(10) Maintain the APMS-AITR module as the official Army inventory of IT capabilities/initiatives, and investigate potential alternatives for a database that can integrate and enhance support to the portfolio management process.

(11) In conjunction with the Assistant Secretary of Defense (Networks and Information Integration) (ASD (NII)), integrate the architectures that support enterprise IT solutions.

(12) Provide Technical Architectures to the Army IT PfM Process.

(13) Provide Departmental level policy, guidance, and direction in the definition, design, implementation, and integration of enterprise solutions and business process improvements across the Army and between the DoD, the Army, and other external organizations.

(14) Serve as the facilitator for the IT Investment Strategy for the PPBE Review Boards promoting IT integration across MAs.

(15) Provide feedback to MA/Domains on lessons learned and best business practices on IT PfM.

(16) Provide a prioritized listing of all IT investments, by MDEP to the PEGs.

***k.* Central Technical Support Facility (CTSF)**

(1) Provide, as appropriate, testing resources IAW the DoD Instruction 4630.8 Para 4., and Army policy.

(2) Serve as the facility that offers systems interoperability, integration testing, configuration management and field engineering to Army Program Managers and System Developers.

***l.* Planning, Programming and Budgeting Committee (PPBC)**

(1) The final authoritative body for resolution of cross-MA PfM issues. The Senior Review Group (SRG) serves as the overarching governance body for integration decisions between GIG ES MA, pertaining to IT Portfolio Investments. SRG responsibilities include:

(a) Resolving resource allocations and other issues;

(b) Monitoring staff implementation of decisions;

(c) Recommending prioritization of programs unresolved at lower levels; and

(d) Recommending resource alternatives.

***m.* MACOMS (General)**

(1) Implement, as required, the IT PfM Process developed by DoD and the Army to define and justify MACOM IT Portfolio capability-focused expenditures.

(2) Utilize the Army PfM tool to determine within MACOMS where capability redundancies exist and where integration of products and services might better support warfighter needs.

(3) Ensure IT capabilities/initiatives are registered in the APMS-AITR module.

(4) Establish and utilize outcome-oriented IT performance measures, (in cooperation with Army Domains), that are aligned with Army Domain strategic guidance.

(5) Ensure MACOM portfolios of capabilities are congruent with applicable MA and Domain strategic plans and portfolios.

***n.* MACOMS (Specific)**

(1) TRADOC, as the Army's combat developer with responsibility to validate requirements with any warfighting impact and to assist DA to prioritize and justify warfighting requirements, assist MA/Domains in the Binning, Criteria Determination, Analyze, Select, and Evaluate Phases of the Army IT PfM Process.

(2) TRADOC develop and enforce Operational Architectures for systems and systems of systems, to support Army IT PfM.

***o.* System Owners/Program Managers (SOs/PMs)**

(1) Ensure all IT investments are entered in APMS and records are accurate and current in mandatory DoD level and other Army repositories as required by policy.

(2) Maintain System Architectures that are compliant with Army Enterprise Architecture (AEA), MA, Domain and other DoD/Joint architectures and policies as appropriate.

(3) Assure compliance with OSD Certification processes through HQDA, CIO/G6 (e.g. Applying to the IRB and DBSMC, via the appropriate headquarters level authority, for system review and certification before obligating development/modernization funds over $1,000,000 for business information systems over the FYDP subject to NDAA required OSD Certification.)

(4) Ensure portfolios of IT capabilities are congruent with applicable MA and Domain strategic plans and portfolios.

(5) Ensure applicable testing requirements are satisfied and reported into APMS.

Chapter 6
Summary

Management of the Army’s IT investments/capabilities as portfolios, capitalizing upon best practices, emerging technology and common solutions is essential to the Army’s transformational efforts. As the Army transforms, it is imperative that IT investment portfolios support the Army’s Mission, Vision, and Strategic Goals; ensure an efficient delivery of capabilities to the Warfighter; and maximize return on investment to the enterprise. At the Enterprise level, management of IT portfolios begins with MAs and Domains aligning functional requirements and capabilities with IT solutions. This will enable the Army to increase efficiency/effectiveness through the elimination/consolidation of redundant or outdated capabilities, and provide increased technical performance. IT Investments must be analyzed and prioritized to maximize strategic alignment and support to the WarFighter.

Appendix A
Expanded Army IT PfM Process and Responsibilities

A-1. Introduction

a. The Army Chief Information Officer (CIO/G6), in coordination with Army Mission Area (MA) and Domain leads, is responsible for developing a formal, structured, repeatable Portfolio Management (PfM) process for Army systems. To facilitate this effort, this document has been designed to articulate the roles, processes, and information needed to determine and continuously adjust the optimum set of Army capabilities needed to support the Business, Warfighter, Enterprise Information Environment (EIE) and Defense Intelligence Mission Areas.

b. For any PfM process to be effective, it must rest upon a solid architecture. The Army Architecture Integration Cell (AAIC) serves as the integrating office for the Army Architecture. Management and oversight of the Army Architecture is the responsibility of the Army CIO/G6 AAIC in conjunction with the G-3/5/7, Chief Architect.

c. This appendix describes the Army IT PfM Process, interfaces, and dependencies between the MA and Domain Leads and the linkages to the overarching business processes (JCIDS, PPBE, DAS).

d. MA/Domain owners were assigned by the Secretary of the Army (SA) and are identified in Figure 1. MA/Domain Leads are those entities that have been assigned by the owners to fulfill the responsibilities described in this document.

A-2. Objectives

a. The objectives of this effort are to define and implement an Army IT PfM process that is repeatable, and produces reliable results. Successful implementation of this process should result in the following outcomes:

(1) Ensure the warfighting force has the best IT capabilities to perform its missions and conduct effective information operations, eliminate outdated ways of doing business and achieve net-centricity goals.

(2) Improve warfighting effectiveness by approaching IT investments/capabilities as a portfolio to minimize risk by balancing opportunity with sound investment strategy within the joint warfighting environment.

(3) Ensure optimal IT implementation to satisfy Domain owner/MA/DA/ASA validated capabilities and mission outcomes.

(4) Implement and integrate Army IT PfM processes and recommendations into the JCIDS, DAS and the PPBE processes. Those IT investments that fall below the threshold of these processes will still be incorporated in the IT PfM Evaluation process.

(5) Ensure generating force efforts are traceable to, and fully support, the required IT capabilities for DoD Warfighting, Intelligence, and EIE Mission Areas.

(6) Reduce IT capabilities/systems duplication and gaps.

(7) Develop and maintain the Army IT capabilities portfolio to include systems, programs, and initiatives.

(8) Ensure portfolios of MA/Domain related systems are rationalized against IT capabilities needed to support the warfighter;

(9) Provide a process that looks across the enterprise to effectively influence investment decisions across the MA/Domain Portfolios; and

(10) Ensure a MA/Domain Portfolio that supports information interoperability and enterprise integration among MA/Domain related systems.

A-3. Army IT Portfolio Management (PfM) Process

a. **Process Overview** Figure A-1 shows an overview of the PfM Process that consists of Binning, Criteria Determination, Analyze, Select, Control, and Evaluate Phases as outlined in DODD 8115.01. The IT PfM Process will result in recommendations to influence JCIDS, the DAS, and the PPBE processes.

Portfolio Management Process

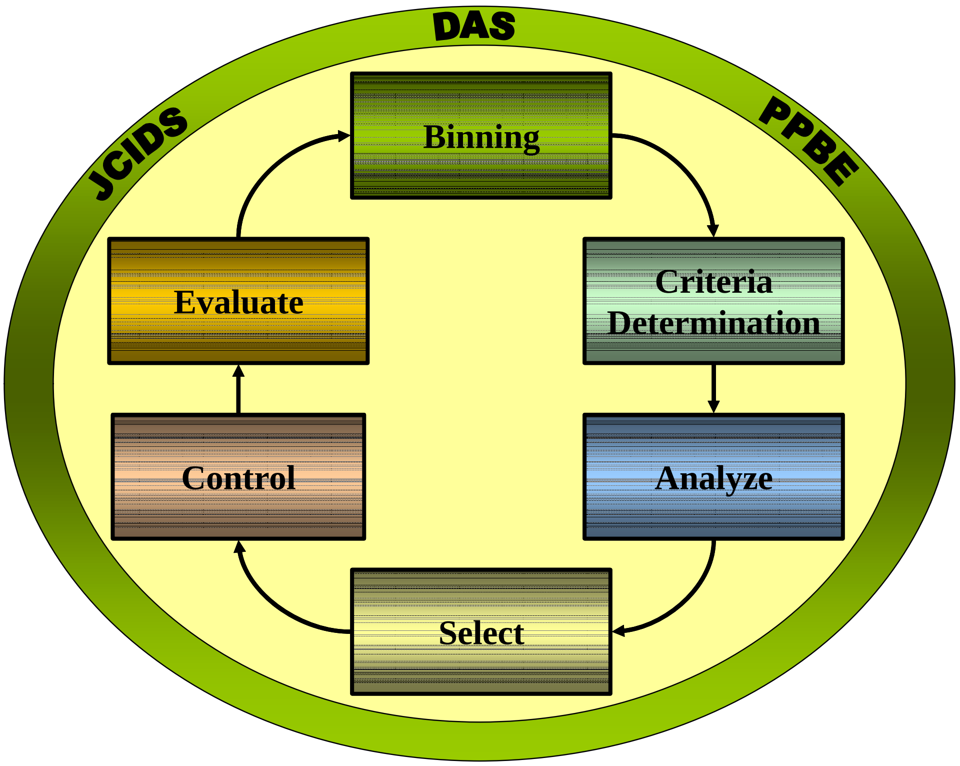


Figure A-1 – Portfolio Management Process

b. A general description of the process' six activities/phases follows with a detailed task break down for each phase. The phases are:

(1) **Binning**. Assign specific capabilities and IT investments to the governing Army IT MA/Domains and collect investment information. IT Domain binning will be synchronized with the Army JCIDS Gatekeeper function.

(2) **Criteria Determination**. Identify portfolio goals, assessment metrics, and risk assessment criteria used to analyze Army IT investments. Criteria determination is typically covered as part of the analyze activity, however it is addressed separately here to highlight its importance.

(3) **Analyze**. Assess and prioritize IT investments against Army MA/Domain criteria. Link portfolio objectives to Enterprise vision, mission, goals, objectives, and priorities; develop

quantifiable outcome-based performance measures; identify capability gaps, opportunities, and redundancies; identify risks; and provide for continuous process improvement.

(4) **Select**. Determine the optimum investment baseline across each Army Domain, MA, cross-MA and propose IT investment baseline changes, including capability identification, acquisition, and funding issues. Identify and select the best mix of IT investments to strengthen and achieve capability goals and objectives for the portfolio and demonstrate the impact of alternative IT investment strategies and funding levels.

(5) **Control**. Ensure a portfolio is managed and monitored using established quantifiable outcome-based performance measures. Portfolios are monitored and evaluated against portfolio performance measures to determine whether to recommend continuation, modification, or termination of individual investments within the portfolio. Forward MA recommendations to the CPIM and Program Owner.

(6) **Evaluate**. Monitor and evaluate IT investment changes that affect the portfolio baseline and appropriately update baseline. Evaluate measures actual contributions of the portfolio against established outcome-based performance measures to determine improved IT capabilities as well as to support adjustments to the mix of portfolio investments, as necessary.

A-4. Binning Phase

Figure A-2 illustrates the Binning Phase. This phase will identify recommended Army IT capabilities/investments and the appropriate MA/Domain Ownership.

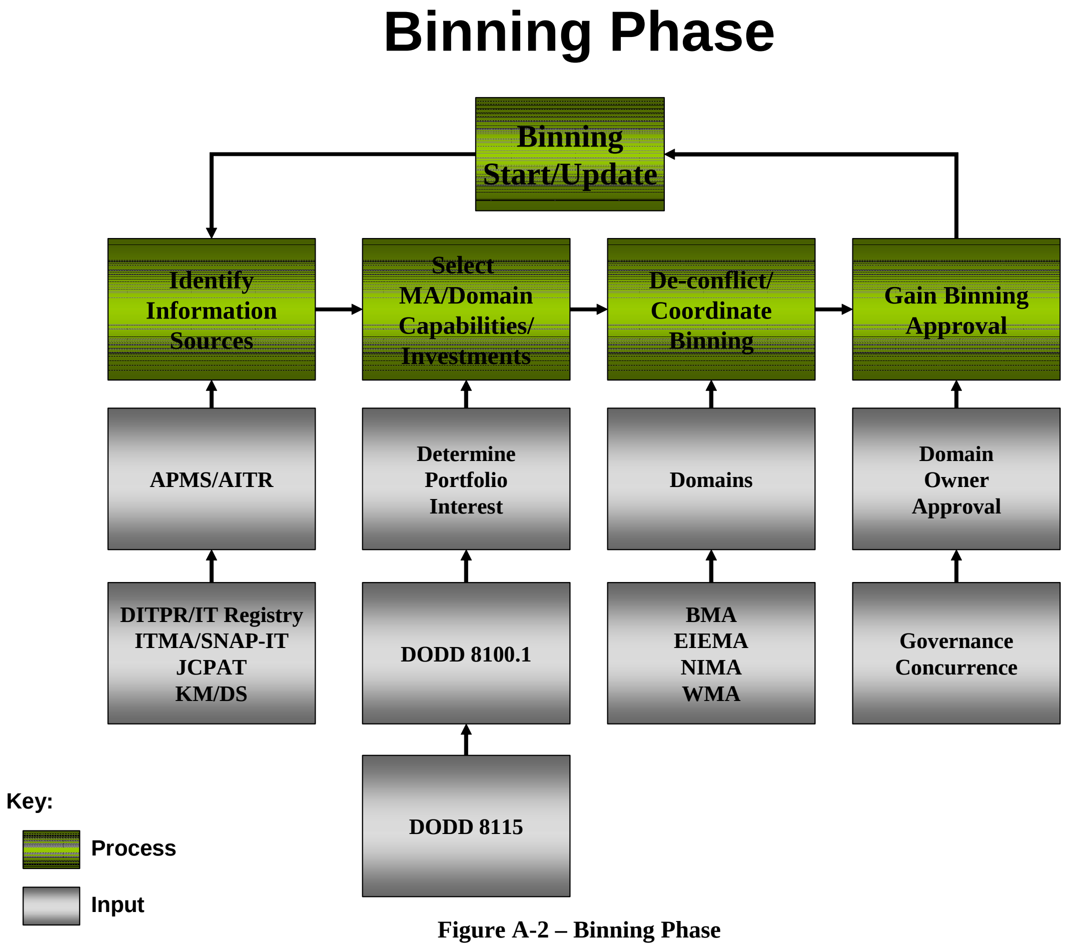


Figure A-2 – Binning Phase

a. **Identify Information Sources.** Domains will ensure that the system owners identify and register all appropriate IT investments/capabilities in APMS. Failure of system owners to register IT investments/capabilities in the appropriate repositories will place funding at risk and may result in removal from Army networks.. Data calls will verify and provide information in the APMS-AITR module.

b. **Select MA/Domain Investments.** The MA/Domain Leads will use the direction in DODD 8115.01, and this guidance, to align IT investments/capabilities to the appropriate Domains. Programs will be added or removed as new IT capabilities are approved or terminated by the appropriate authority.

c. **De-conflict/Coordinate Binning.** After the initial MA/Domain IT portfolio recommendation is developed and Domain assigned, it must be de-conflicted with other MAs and Domains. Each IT investment can be associated with a primary and secondary MAs and Domains, but only one primary MA and Domain may exist for each investment. The Lead Domain will coordinate with the other Domain and MA leads to deconflict assigned MA/Domain. When necessary, the Lead Domain adjudicates among the Domain Owners regarding MA/Domain issues. MA/Domain Owners will monitor and accept or reject requested APMS Domain changes. The Domain Owners will coordinate binning and transfers of IT investments between MAs and Domains.

d. **Mission Area and Domain Assignment Binning Approval.** The Domain Lead will finalize a consolidated Domain IT portfolio binning list and will obtain approval from the Domain Owner. The MA Lead will consolidate the approved Domain Portfolios and gain approval from the MA Owner. Each MA will submit to the APRC their approved Portfolio binning list for approval. Binning will be an iterative on-going process to account for IT investments/capabilities.

A-5. Criteria Determination Phase

The MA/Domains/MACOMs will develop criteria to accomplish the IT PfM objectives in paragraph A-2. Figure A-3 illustrates the Criteria Determination Phase. MA/Domains will establish quantifiable outcome-based performance measures to provide intended IT capabilities. Examples of Army IT Metrics are presented in Appendix C.

a. **Identify Strategic Objectives.** The MA/Domain will develop strategic IT portfolio objectives. The strategic objectives will most likely be common across the MA/Domains. Strategic objectives will incorporate input from the DoD and Army IT strategic plans, TAP, other Strategic Guidance, the National Military Strategy, the Joint Capability Areas (JCAs) and the Quadrennial Defense Review. The MA/Domain objectives should be limited in scope to apply specifically to IT investments within the context of the Army IT PfM for the joint warfighting environment.

b. **Create Portfolio Goals.** DoD and Army strategic objectives are the baseline for developing MA/Domain IT PfM objectives. MA/Domain Owners will develop specific goals to select the best IT investment mix to achieve these objectives. The goals should address short and long-term IT investments. The goals should implement ASD/DCIO direction to increase and report on the use of commercial software and services (ASD/DCIO Memo, Accelerating the use of IT/NSS Commercial Off the Shelf (COTS) Software and Services, 29 Sep 05). Portfolio goals should be reviewed and updated at least annually. Again, the goals should link to the approved JCAs and synchronized with the JCIDS/PPBE/DAS processes. They should also reflect GIG integrated architecture goals. MA/Domain portfolio goals will be briefed to the APRC as background and context for all IT investment recommendations.

c. **Establish Risk Criteria.** MAs will lead the Domain Owners in identifying criteria to assess IT investment risk. Domain Owners may also develop specific Domain criteria that reflect their individual Domain goals. Examples of risk criteria include program funding, staffing available, technology risk, schedule, operational impact, IT investment scope, organizational risk, compliance with GIG architecture standards, use of COTS software, and dependencies on other IT investments. The Domain risk criteria should be coordinated with the associated MA lead to ensure MA goals are accurately reflected in the criteria.

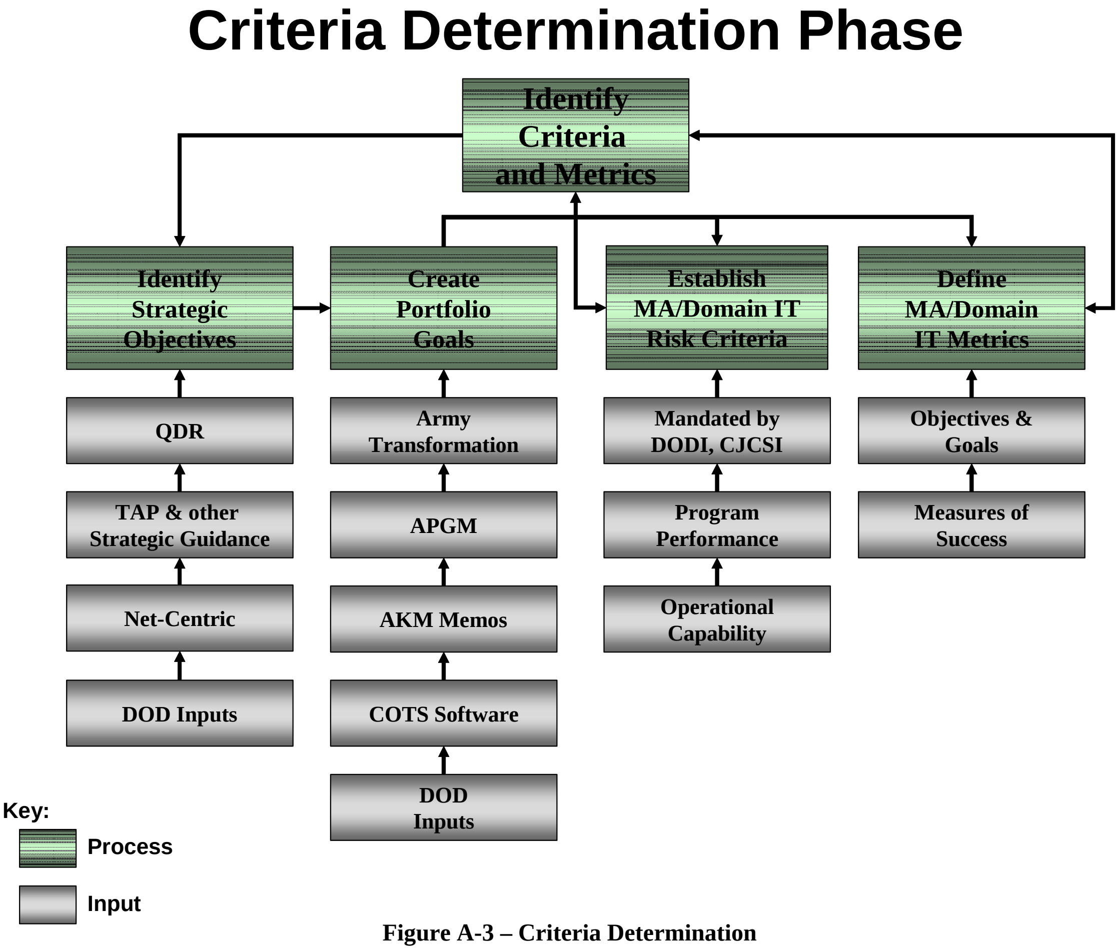


Figure A-3 – Criteria Determination

d. **Define Metrics.** Metrics allow IT investments to be quantitatively and qualitatively evaluated. Metrics can cover mandatory compliance areas, innovation and use of technology, use of Net-Centric tenets, standards and interoperability compliance, mission accomplishment, etc. Some metrics can be collected from existing repositories such as Net-Centric reviews and Information Support Plans. The MA will lead the Domain Owners in identifying metrics to measure whether MA IT investments successfully meet their goals and objectives. A common metrics set will be applied to all Domains IT investments; however, the Domain Owners may develop metrics appropriate to their Domain. CIO/G-6 will develop a common set of metrics for all MAs as indicated in Appendix C. As with the risk criteria, the metrics should be coordinated with the associated MA lead to ensure MA goals are accurately reflected. The metrics should also include the systems ability to comply with GIG integrated architecture standards.

e. IT PfM metrics and criteria will be annually reviewed and approved by the MA/Domains and the APRC.

A-6. Capabilities and Investment Analysis Phases

The next step in the PfM Process is analyzing and prioritizing Army IT assets in relation to the criteria and metrics discussed above and the BMMP and JCA capabilities analysis results. Figure A-4 is the summary view of the JCIDS process and A-5 illustrate the MA/Domain Owner's Investment Analysis Phase.

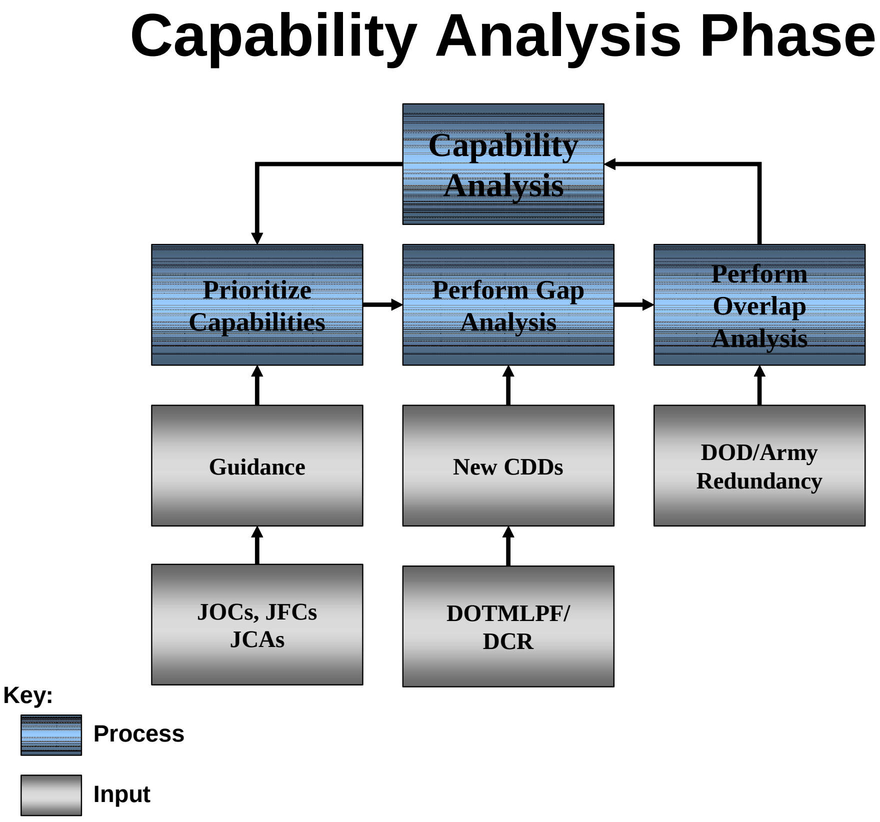


Figure A-4 – Capability Analysis Phase

MA/Domain Leads will use the JCIDS products (which are the outcome of the process described from Figure A-4) IAW CJCSI 3170.01E to ensure linkage of IT investments to capabilities as depicted in Figure A-5.

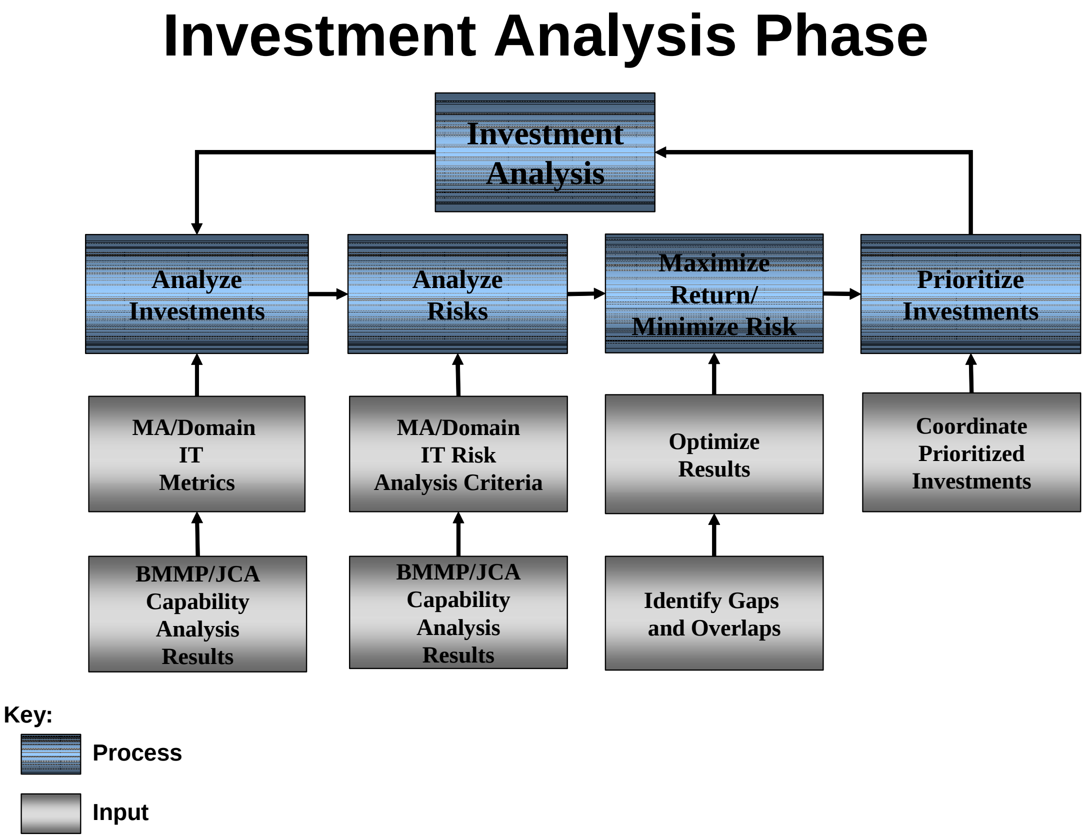

Investment Analysis Phase
Investment Analysis
Analyze Investments
Analyze Risks
Maximize Return/ Minimize Risk
Prioritize Investments
MA/Domain IT Metrics
MA/Domain IT Risk Analysis Criteria
Optimize Results
Coordinate Prioritized Investments
BMMP/JCA Capability Analysis Results
BMMP/JCA Capability Analysis Results
Identify Gaps and Overlaps
Key:
Process
Input

Figure A-5 – Investment Analysis Phase

a. **Investment and Risk Analysis.** The goal of IT investment and risk analysis is to identify investment gaps and overlaps, to determine the optimum MA/Domain portfolio, and to maximize return on investments while minimizing portfolio risk. The MA/Domain Leads, in conjunction with the PEGs, TRADOC, G-8, and ASA(AL&T), will review each IT investment against the capabilities obtained from the capability analysis phase and known requirements. This will include a risk analysis based upon a set of defined criteria. The resulting outcome will be used to evaluate whether the investments are meeting their objectives, and at what level of risk.

b. **Maximize Return/Minimize Risk.** Since the MA/Domain Owner's goal is to maximize return on IT investments while minimizing the overall risk of the portfolio, they must continually evolve their portfolio investment mix in a spiral methodology over time and analyze the portfolio based upon performance and cost metrics to optimize their IT investment portfolio.

c. **Coordinating Recommended MA/Domain IT Priorities.** The MA/Domain Leads will coordinate their recommended portfolio priorities with stakeholders to include the G-3/5/7 and G-8 proponents as required.

d. **Prioritized Investment Portfolio.** The final stage of the IT Investment Analysis phase is for the MA/Domain Owner to prioritize their investments. The resulting recommended prioritized IT investment portfolio will be used to select investments against available financial resources. The prioritized investment list will be used in the Investment Selection Phase.

A-7. Investment Selection Phase

The Investment Selection Phase shown in Figure A-6 will use the prioritized analysis results to determine IT investment funding recommendations and prioritization.

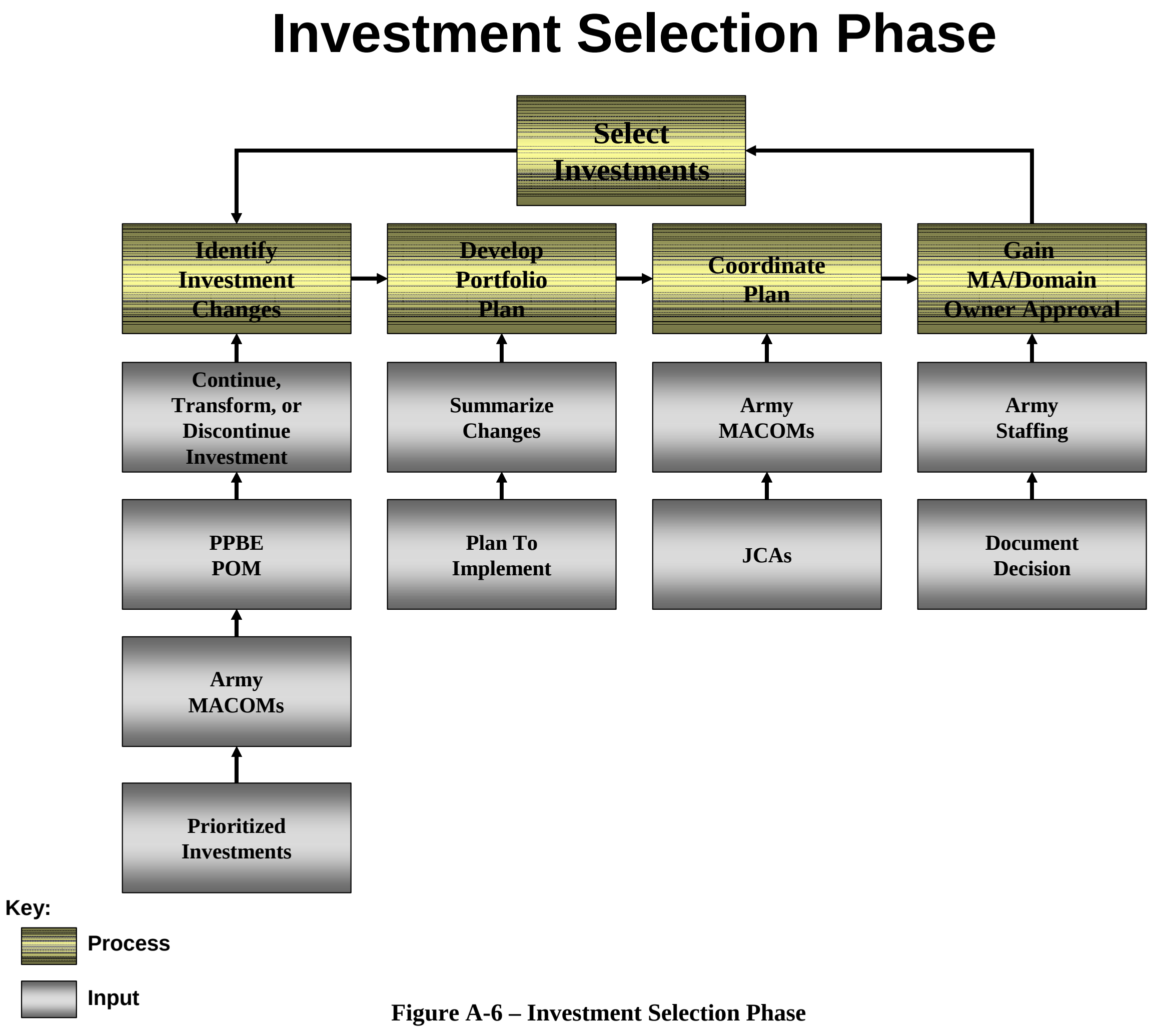


Figure A-6 – Investment Selection Phase

a. **Identify Investment Changes.** The MA/Domain Owner, working in collaboration with system proponents, will identify changes in potential IT investments to be considered in the PPBE process/Program Objective Memorandum (POM). System proponents should analyze recommended investment changes against available resources to acquire needed operational capability. Investments can be continued unchanged, modified, and transformed by combining or discontinuing investments. The recommended investment changes should reflect the analysis results discussed in Figure A-6.

b. **Domain Disconnects.** If multiple Domains have interest in an IT investment, the primary Domain Lead assigned during binning will coordinate the recommended changes with secondary Domains. The primary Domain Lead is responsible for gaining consensus on the recommended change. When consensus cannot be reached, the Domain Lead will develop a recommended best course of action, noting dissenting comments, and forward the recommendation to the MA for resolution.

c. **Develop Portfolio Plan.** Once IT investment changes are identified, a portfolio plan will be developed. The plan will list and summarize recommended changes to the portfolio baseline with appropriate rationale. Only the recommended changes need to be mentioned unless additional information will clarify the overall results. As required, the CIO/G-6 will provide a portfolio plan template to the MA/Domain Owners for use in reporting their investment selection results.

d. **Coordinate Plan.** The MA/Domains will coordinate the portfolio plan with all stakeholders and other interested organizations for comment as required. When coordination is complete, the MA/Domain staff will adjudicate the comments and update the plan in preparation for MA/Domain Lead approval.

e. **Domain Owner Approval.** When coordination is complete, the MA/Domain Owner will attain approval of the coordinated portfolio plan from Army Leadership as required. The approval will be documented in a memo and provided to CIO/G-6, ASA(AL&T), and PEG Executives. The MA/Domain Owner will also input the portfolio plan results into APMS.

A-8. Investment Control Phase

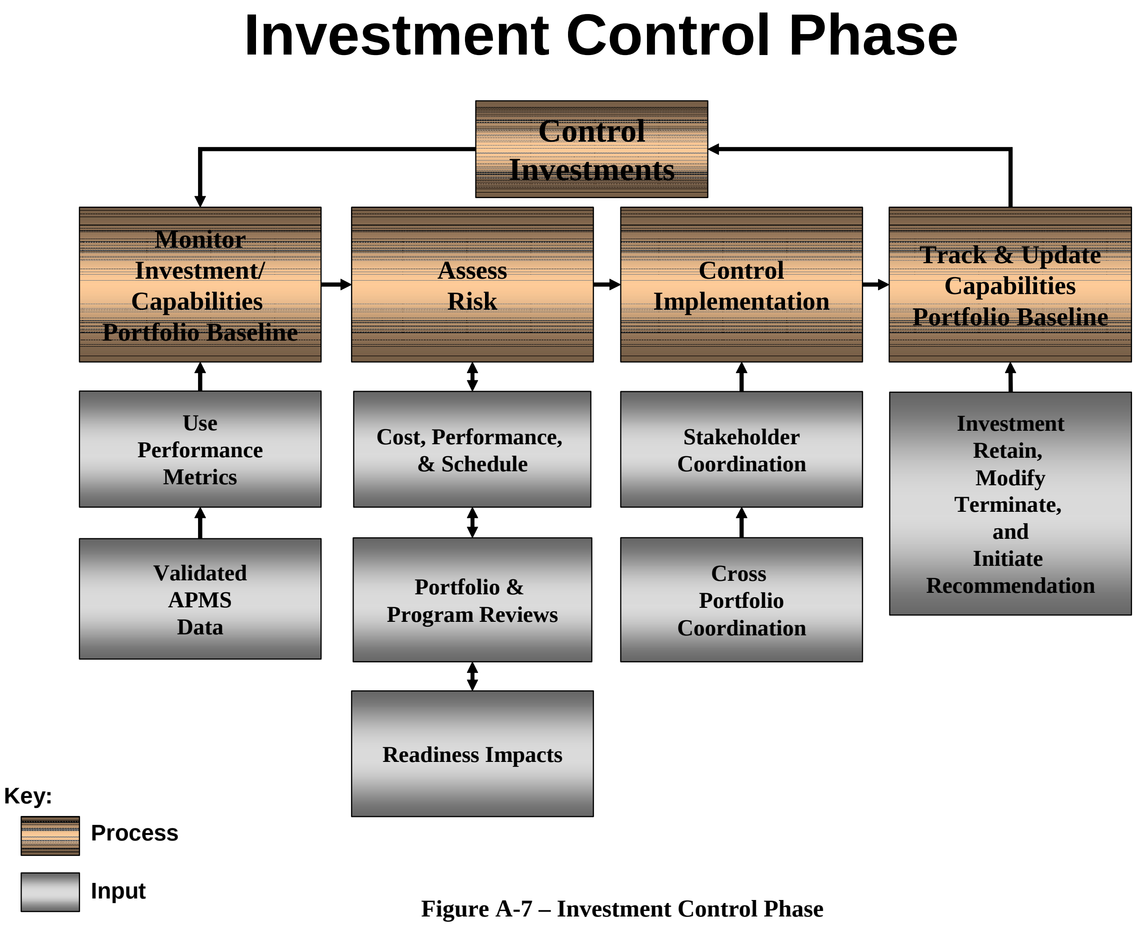

Investment Control Phase
Control Investments
Monitor Investment/ Capabilities Portfolio Baseline
Assess Risk
Control Implementation
Track & Update Capabilities Portfolio Baseline
Use Performance Metrics
Validated APMS Data
Cost, Performance, & Schedule
Portfolio & Program Reviews
Readiness Impacts
Stakeholder Coordination
Cross Portfolio Coordination
Investment Retain, Modify Terminate, and Initiate Recommendation
Key:
Process
Input

Figure A-7 – Investment Control Phase

a. Figure A-7 illustrates the Investment Control Phase. The MA/Domain Owners will implement their portfolio plan to ensure the warfighting force has the best IT capabilities to perform its missions and conduct effective information operations, eliminate outdated ways of doing business and achieve net-centricity goals. Within the IT PfM Process, the MA/Domains will:

(1) With the appropriate Army entities, represent the MA/Domain's IT capability and resource needs and priorities within the PPBE, DAS, and JCIDS processes.

(2) In conjunction with G-3/5/7, CIO/G-6, G-8 and ASA(AL&T) processes, manage and routinely monitor the performance of all current and planned IT investments within the Domain.

(3) Make recommendations through existing processes on which IT investments to retain, modify, terminate and initiate based on the GIG integrated architecture, MA goals, risk tolerance levels, potential returns and performance.

b. By managing IT investments as portfolios, MA/Domain Owners should be able to ensure IT investments support the Army's vision, mission, and goals; to ensure efficient and effective delivery of capabilities to the warfighter; and to maximize return on investment to the Enterprise. This is the heart of the Army IT PfM Process.

c. During the Control Phase, which is ongoing, program execution is monitored to ensure that approved mission benefits, cost, schedule, and performance baselines remain attainable. If these parameters are unable to be attained or are projected to be unacceptable within the approved program baseline, the IT investment/capability must be reevaluated under the Select Phase and established selection criteria. Accordingly, requirements, planning parameters, and resources should be realigned to revise the program baseline. MA and Domain Leads will:

(1) **Monitor Investment/Capabilities Portfolio Baseline**

(a) Establish and utilize outcome-oriented IT performance measures.

(b) Ensure program information is entered, accurate and current in APMS.

(2) **Assess Risk**

(a) Review cost, performance & schedule

(b) Utilize APMS tool to assist in determining where redundancies exist and where integration of products and services might better support warfighter needs.

(c) Utilize data from on-going Army program/project reviews as conducted by MACOMs, ASA(AL&T) and G-8 among other sources to support risk assessment

(d) Review Readiness Impacts based upon recommendations to retain, modify, terminate or initiate.

(3) **Control Implementation**

(a) De-conflict with other MAs/Domains.

(b) Stakeholder coordination

(c) Cross portfolio coordination

(4) **Track & Update Capabilities Portfolio Baseline** - Recommend IT Portfolio Investments (retain, modify, terminate, initiate recommendations) in support of JCIDS, DAS, and PPBE.

A-9. Portfolio Evaluation Phase

Figure A-8 depicts the Portfolio Evaluation Phase. Investment evaluation consists of monitoring change recommendations, ensuring they are consistent with MA/Domain Owner portfolio recommendations, and updating the PfM record systems.

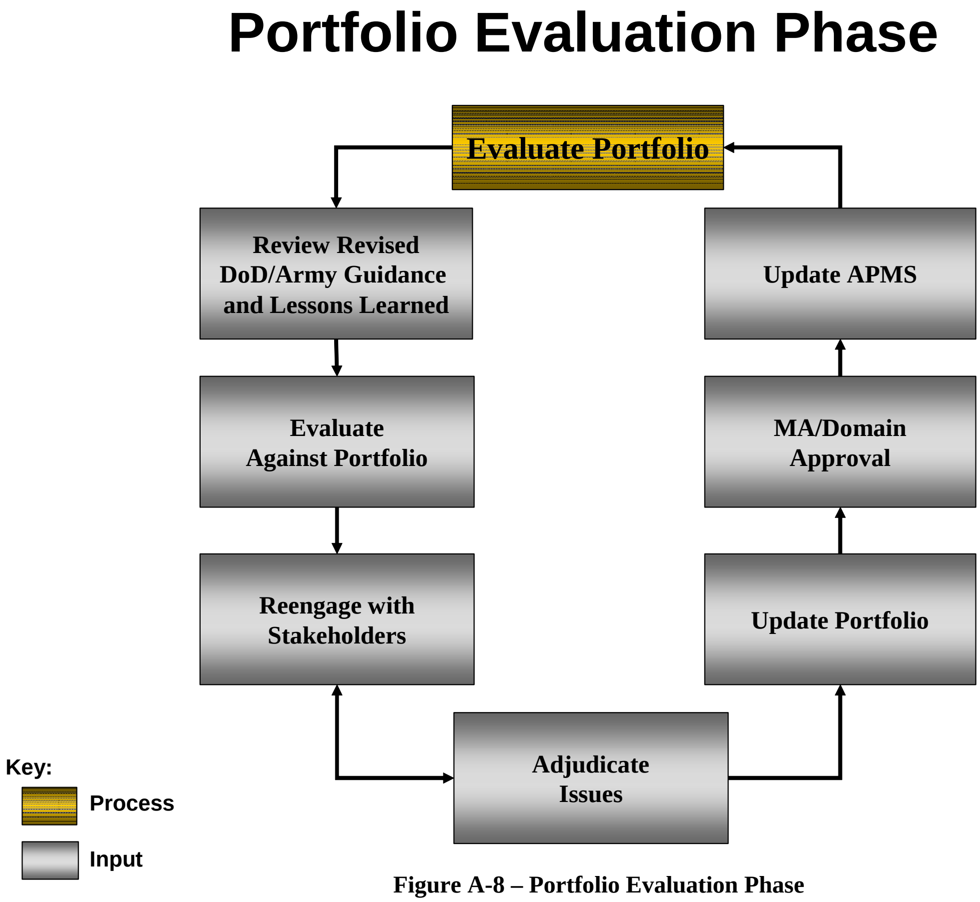

Portfolio Evaluation Phase
Evaluate Portfolio
Review Revised DoD/Army Guidance and Lessons Learned
Evaluate Against Portfolio
Reengage with Stakeholders
Adjudicate Issues
Update Portfolio
MA/Domain Approval
Update APMS
Key:
Process
Input

Figure A-8 – Portfolio Evaluation Phase

a. **Review IT Investment Change Documentation.** The MA/Domain Leads will monitor and review DoD/Army guidance (for example, Program Budget Decisions (PBDs), JROC, other Program Objective Memorandum (POM) documents, etc.) and lessons learned.

b. **Evaluate Against Portfolio.** The MA/Domain Leads will evaluate the guidance documents to determine if recommendations were implemented. As issues are generated, the MA/Domain Leads will also monitor required changes.

c. **Reengage with Stakeholders.** MA/Domain Leads will reengage with stakeholders to determine the impact level on their required IT capabilities/investments.

d. **Adjudicate Issues.** MA/Domains will adjudicate as necessary.

e. **MA/Domain Approval.** The MA/Domains will update and approve the portfolio information for all their IT investments/capabilities and make necessary adjustments to MA/Domain strategy and plans.

f. **Update APMS.** This may require updates to the APMS-AITR module or other modules within the APMS.

A-10. Summary

This is not a static process but is a fluid and dynamic one built upon repeatable steps. MA/Domain Leads must constantly review and reevaluate portfolios based upon evolving guidance. The effort of the Analyze, Select, Control & Evaluate Phases is to support the POM process.

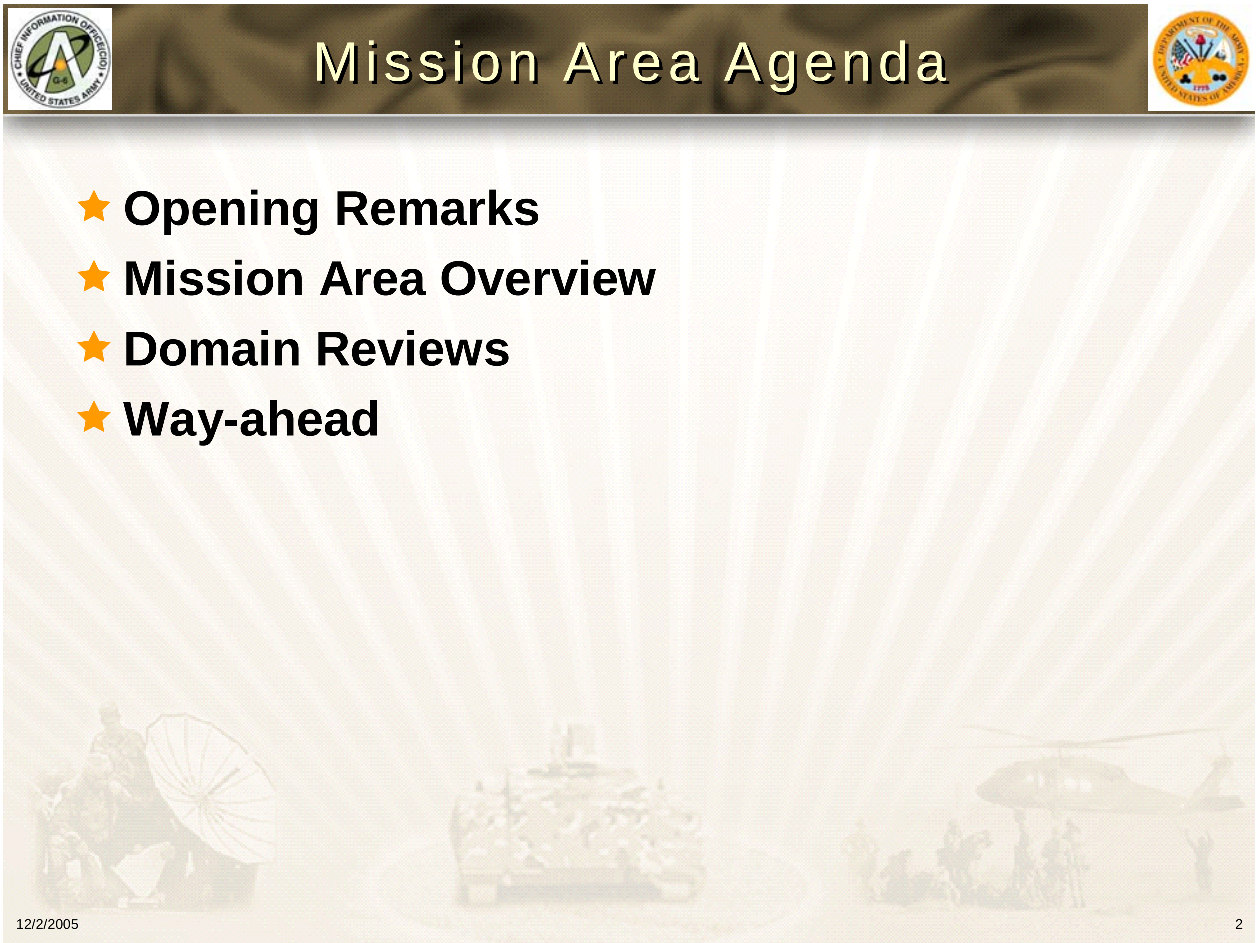
Appendix B
Mission Area/Domain Portfolio Review Requirements

The MA/Domains will provide appropriate briefers (SME/POC/PM) for each system being reviewed by the APRC. Domains will provide, for each system being reviewed, all required briefing materials on AKO as required.

B-1. Mission Area Agenda

(Use template provided in Figure B.1 below)

a. Provide Opening Remarks
b. Provide Mission Area Overview
c. Provide Domain Reviews
d. Provide Mission Area Way-Ahead



Mission Area Agenda

- ★ Opening Remarks
- ★ Mission Area Overview
- ★ Domain Reviews
- ★ Way-ahead

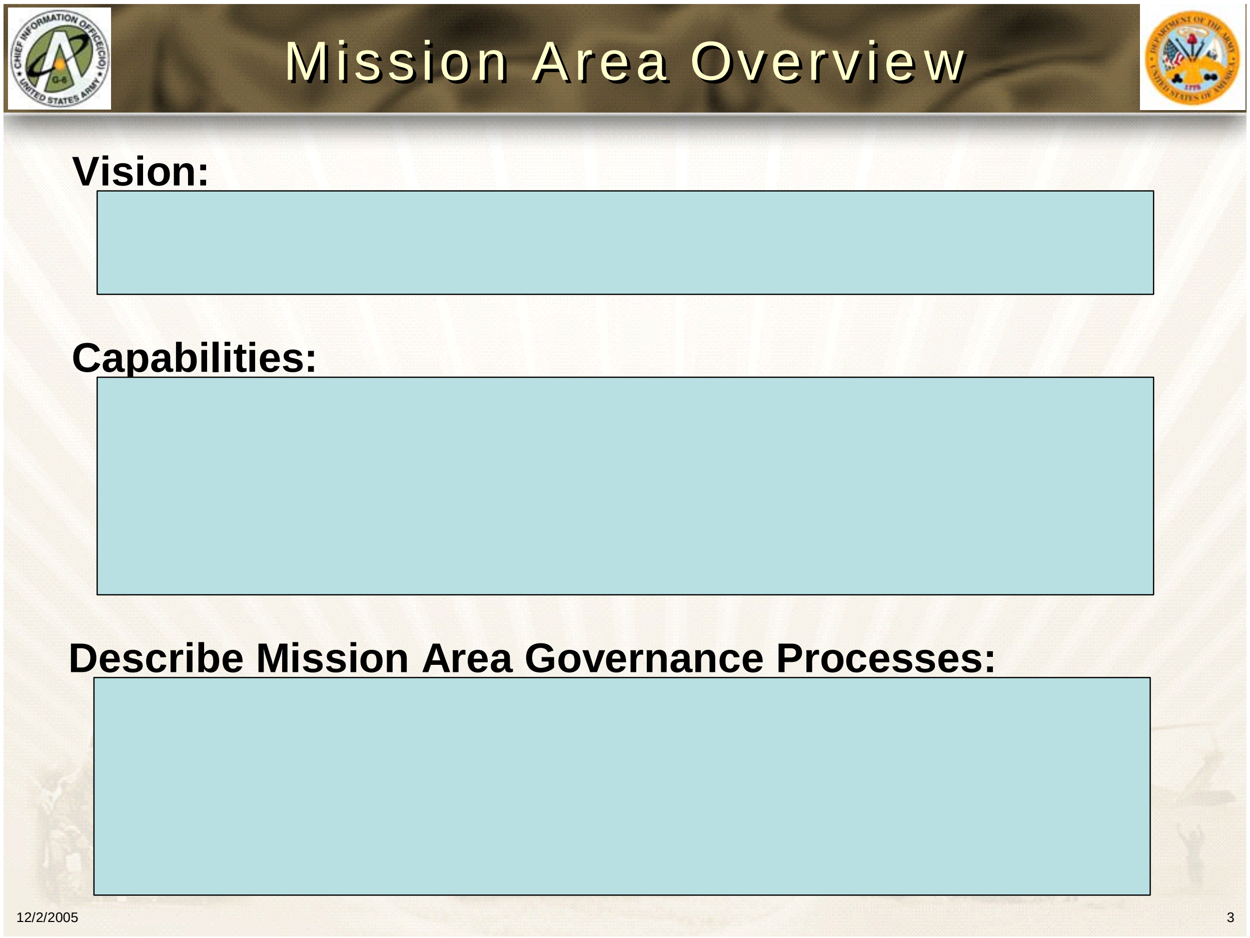
12/2/2005 2

Figure B.1 – Mission Area Agenda

B-2. Mission Area Overview

(Use template provided in Figure B.2 below)

a. Provide the Mission Area's vision.
b. Provide the Mission Area's major IT capabilities.
c. Describe Mission Area governance processes used to identify and manage IT investments.



Mission Area Overview

Vision:

Capabilities:

Describe Mission Area Governance Processes:

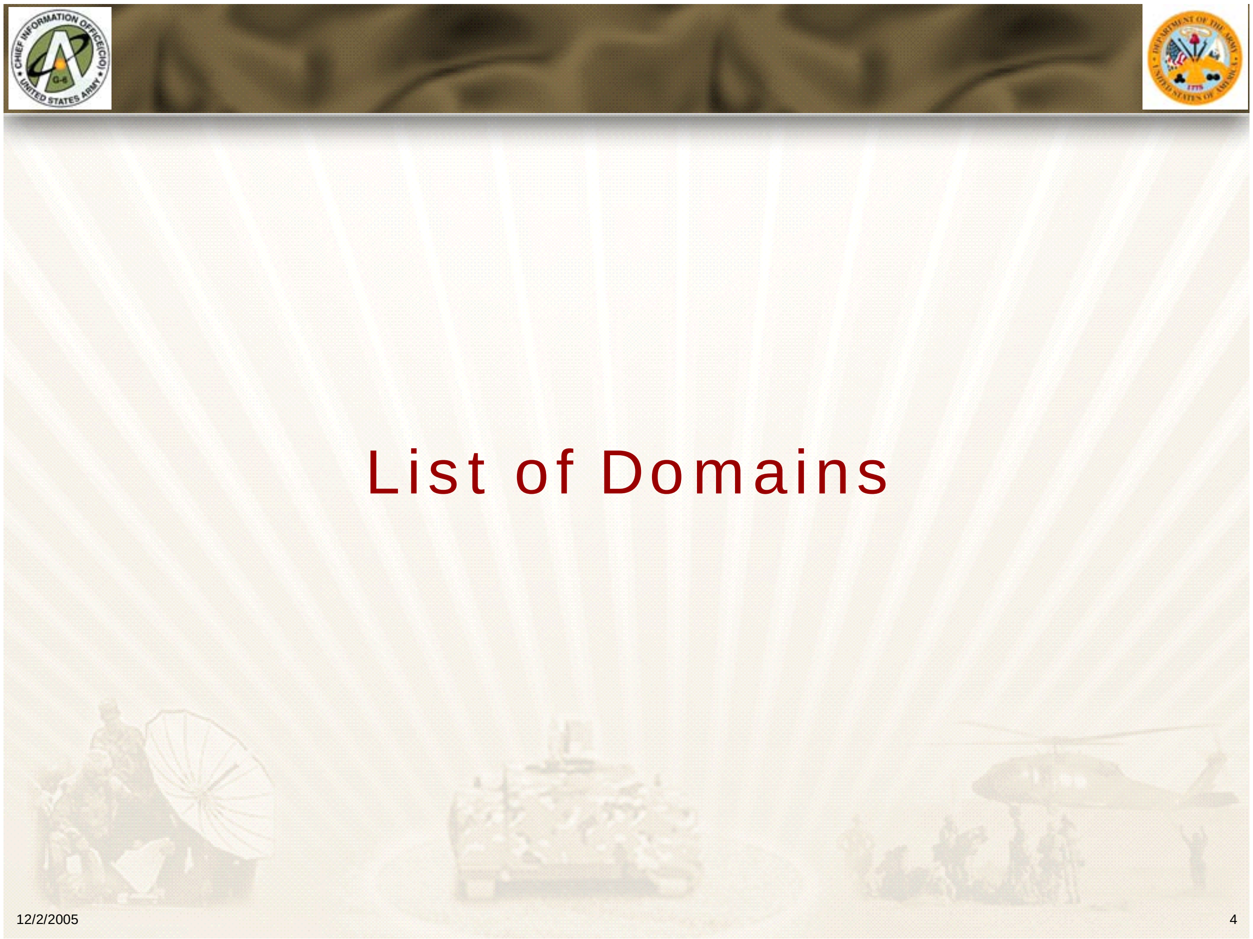
12/2/2005

3

Figure B.2 – Mission Area Overview

B-3. List of Domains – The MAs will provide a list of their Domains.

(Use template provided in Figure B.3 below)



List of Domains

12/2/2005

4

Figure B.3 – List of Domains

B-4. Domain IT Portfolio Review Agenda – The following areas will be briefed for each Domain being reviewed.

(Use template provided in Figure B.4 below)

a. Domain Vision

b. Capabilities - Identify Core, Legacy, and Interim IT Capabilities and Investments

c. Governance Processes

d. Overview of Plan/Timeline to Reduce/Eliminate 80% Duplicate Capabilities

e. Status of Information Assurance (FISMA compliance)

f. Strategy for Interoperability Testing, Integration, and Configuration Management at CTSF

g. Domain PfM Transformation Schedule

(1) E.g. Identify Timeline for legacy sunset dates and determine when and/or if interim capabilities will transition to core or terminate

h. Portfolio Review Dashboard

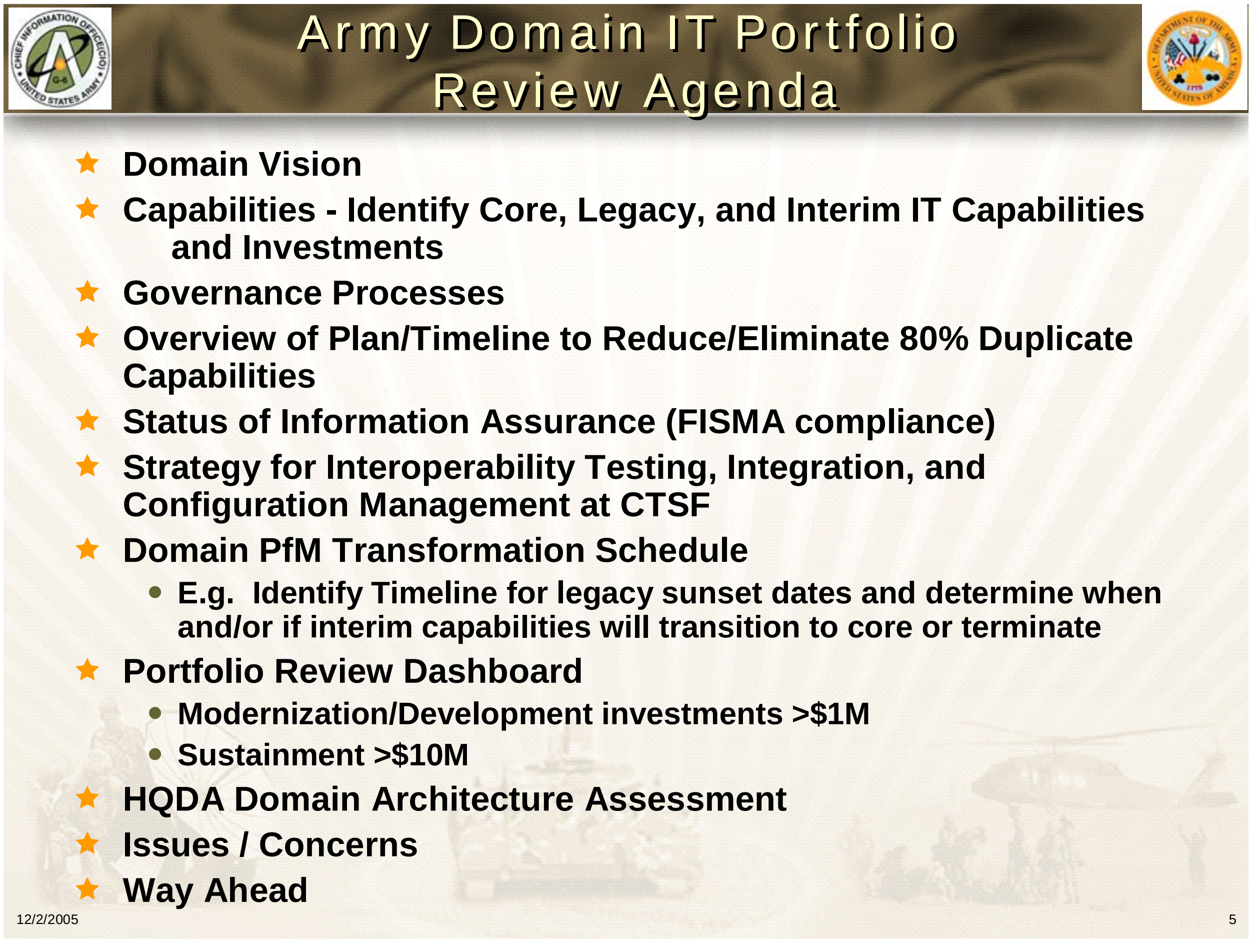
i. Modernization/Development investments >$1M

j. Sustainment >$10M

k. HQDA Domain Architecture Assessment

l. Issues / Concerns

m. Way Ahead



Army Domain IT Portfolio Review Agenda

- ★ Domain Vision
- ★ Capabilities - Identify Core, Legacy, and Interim IT Capabilities and Investments
- ★ Governance Processes
- ★ Overview of Plan/Timeline to Reduce/Eliminate 80% Duplicate Capabilities
- ★ Status of Information Assurance (FISMA compliance)
- ★ Strategy for Interoperability Testing, Integration, and Configuration Management at CTSF
- ★ Domain PfM Transformation Schedule
  - E.g. Identify Timeline for legacy sunset dates and determine when and/or if interim capabilities will transition to core or terminate
- ★ Portfolio Review Dashboard
  - Modernization/Development investments >$1M
  - Sustainment >$10M
- ★ HQDA Domain Architecture Assessment
- ★ Issues / Concerns
- ★ Way Ahead

12/2/2005 5

Figure B.4 – Domain IT Portfolio Review Agenda

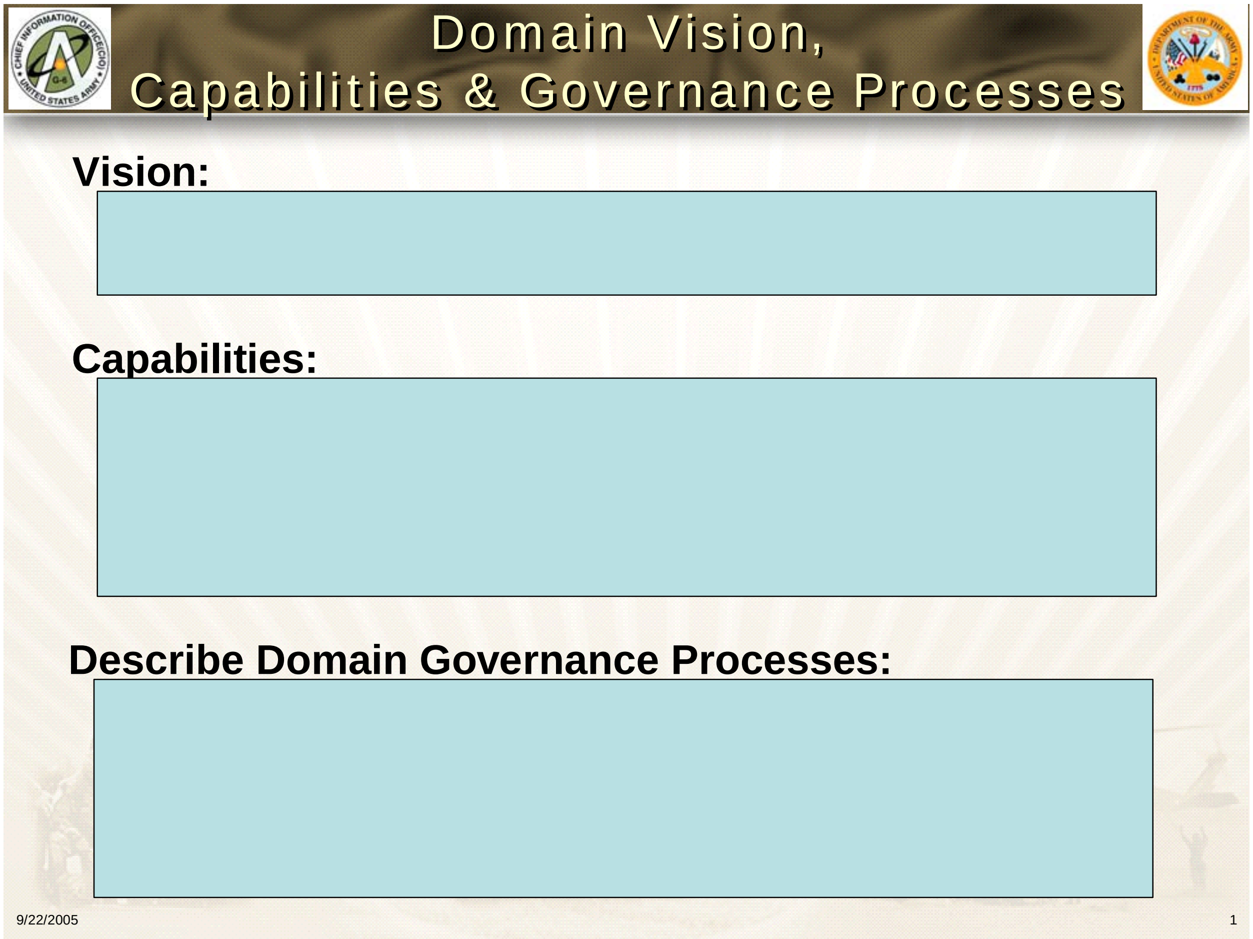
B-5. Domain Vision, Capabilities, and Governance Processes

(Use template provided in Figure B.5 below)

a. Provide the Domain's vision.

b. Provide the Domain's major IT capabilities.

c. Describe Domain governance processes used to identify and manage IT investments.



Domain Vision,
Capabilities & Governance Processes

Vision:

Capabilities:

Describe Domain Governance Processes:

9/22/2005

1

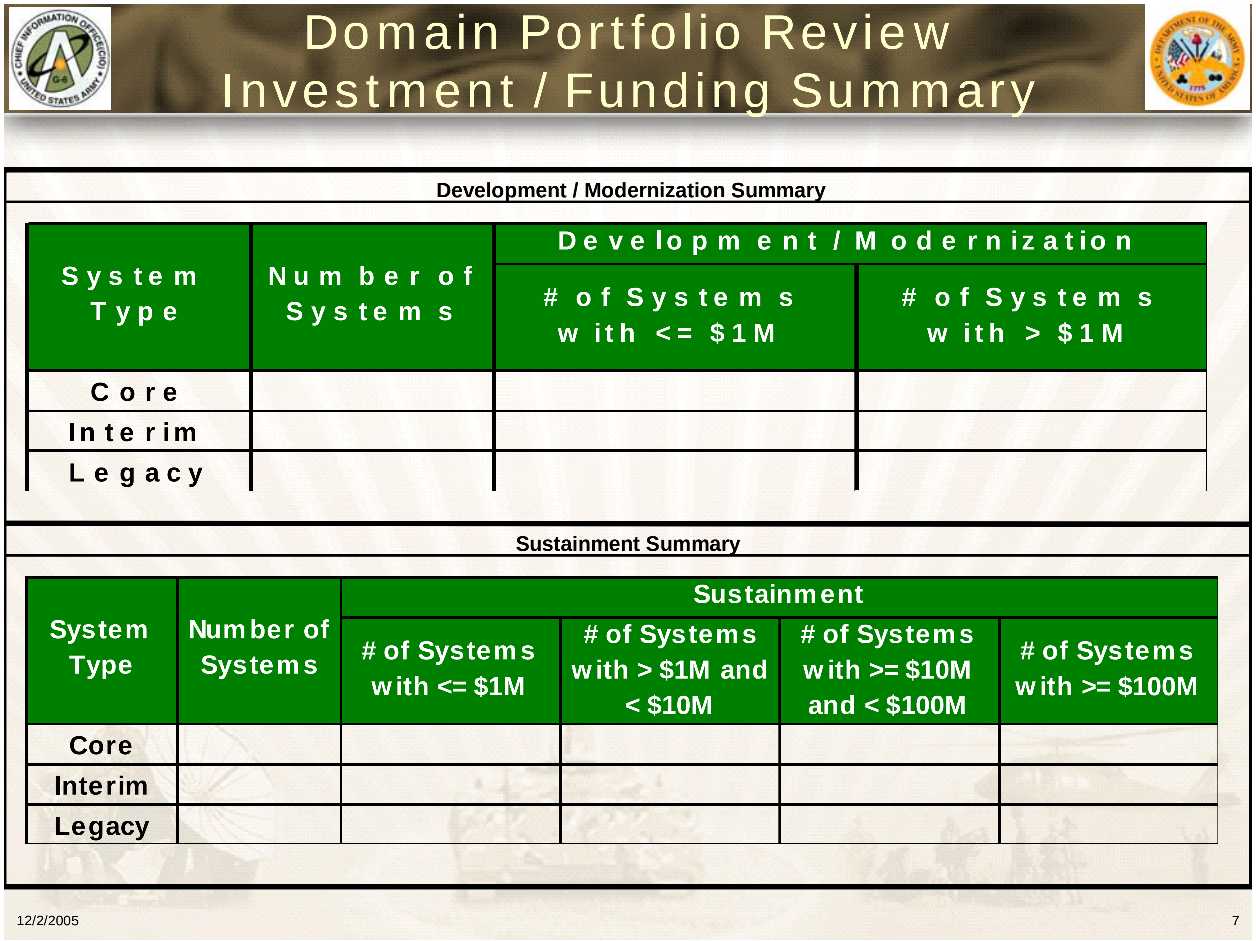
Figure B.5 – Domain Vision, Capabilities, and Governance Processes

B-6. Domain Portfolio Review Investment / Funding Summary

(Use template provided in Figure B.6 below)

a. Identify the number of systems for each system type (Core, Interim, Legacy) under each Dev/Mod funding range (<= $1M, > $1M).

b. Identify the number of systems for each system type (Core, Interim, Legacy) under each Sustainment funding range (<= $1M, > $1M and < $10M, >= $10M and < $100M, >= $100M).



Domain Portfolio Review Investment / Funding Summary

Development / Modernization Summary

System Type	Number of Systems	Development / Modernization	
		# of Systems with <= $1M	# of Systems with > $1M
Core			
Interim			
Legacy			

Sustainment Summary

System Type	Number of Systems	Sustainment			
		# of Systems with <= $1M	# of Systems with > $1M and < $10M	# of Systems with >= $10M and < $100M	# of Systems with >= $100M
Core					
Interim					
Legacy					

12/2/2005

7

Figure B.6 – Domain Portfolio Review Investment / Funding Summary

B-7. Domain Portfolio Review Information Assurance Summary

(Use template provided in Figure B.7 below)

a. With support from NETCOM, provide the status on Domain Systems in meeting FISMA requirements for certification and accreditation, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) to include:

(1) % of systems certified and accredited (full Authority To Operate (ATO)),

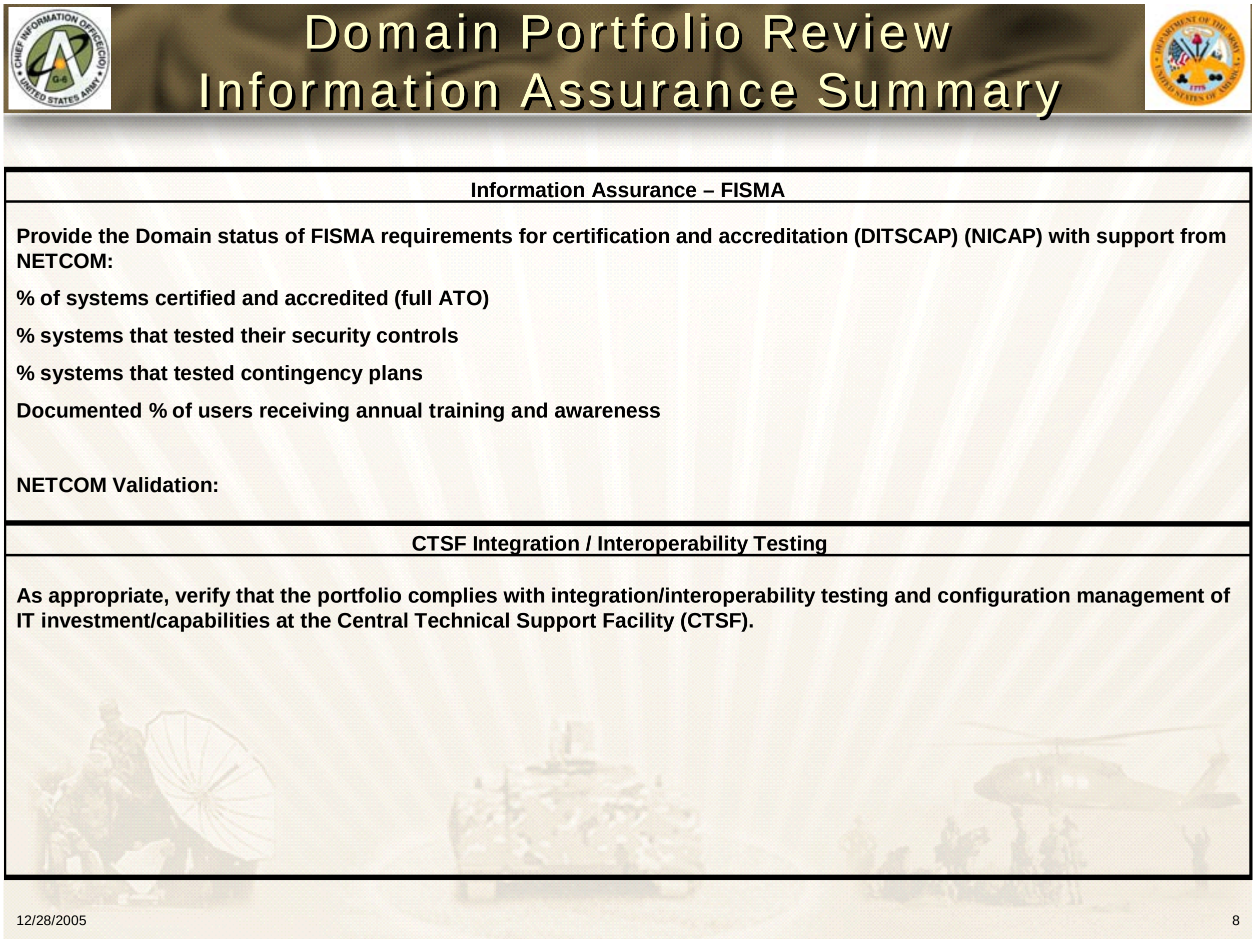
(2) % systems that tested their security controls,

(3) % systems that tested contingency plans,

(4) Documented % of users receiving annual training and awareness, and

(5) NETCOM Validation.

b. As appropriate, verify that the portfolio complies with integration/interoperability testing and configuration management of IT investment/capabilities at the Central Technical Support Facility (CTSF).



Domain Portfolio Review
Information Assurance Summary

Information Assurance – FISMA

Provide the Domain status of FISMA requirements for certification and accreditation (DITSCAP) (NICAP) with support from NETCOM:

% of systems certified and accredited (full ATO)

% systems that tested their security controls

% systems that tested contingency plans

Documented % of users receiving annual training and awareness

NETCOM Validation:

CTSF Integration / Interoperability Testing

As appropriate, verify that the portfolio complies with integration/interoperability testing and configuration management of IT investment/capabilities at the Central Technical Support Facility (CTSF).

12/28/2005 8

Figure B.7 – Domain Portfolio Review Information Assurance Summary

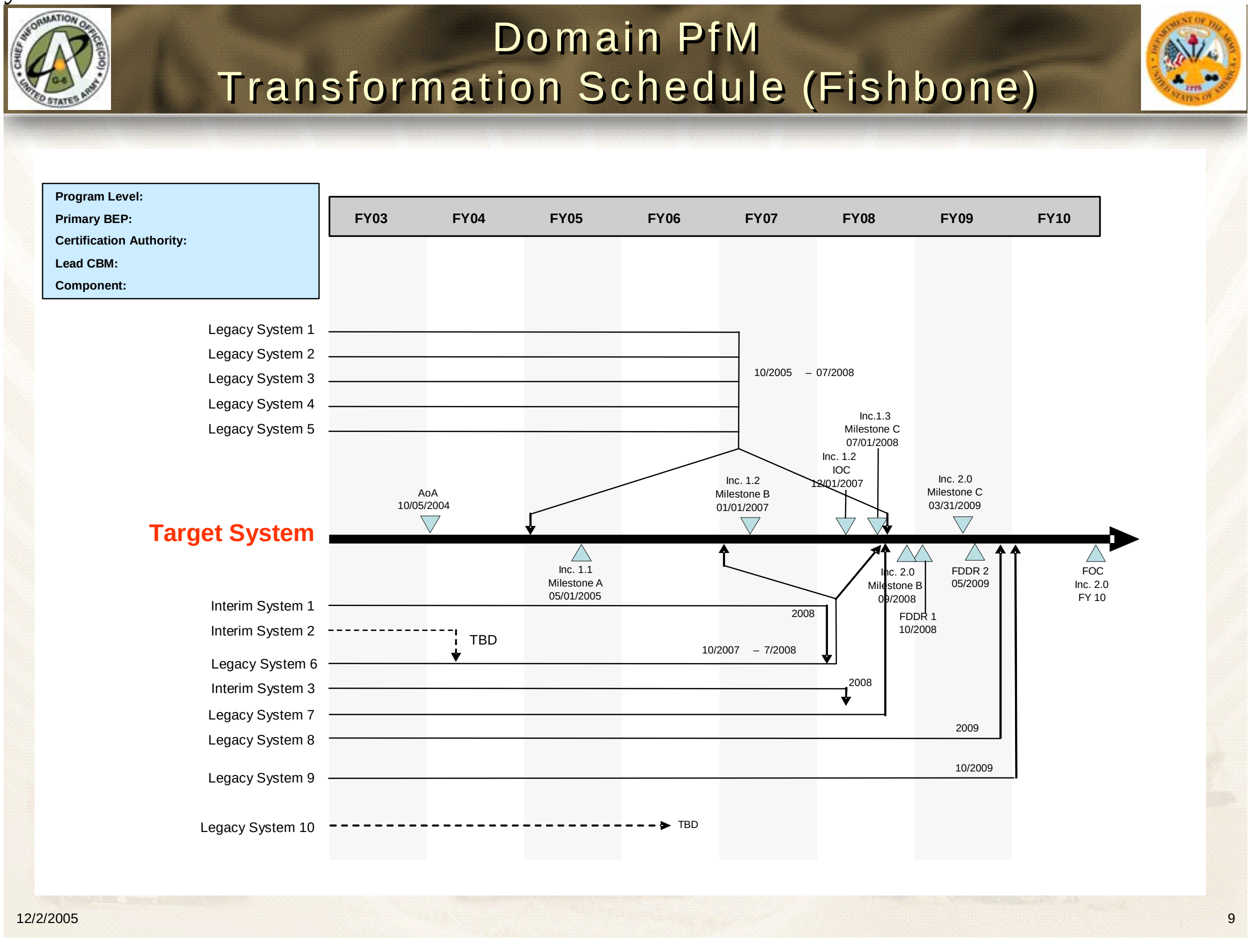
B-8. Domain PfM Transformation Schedule

(Use template provided in Figure B.8 below)

a. For each Domain Target IT system, the Domain will provide an overview graphic of systems transformation/replacement of legacy systems, to interim solutions, to future target systems. The fishbone diagram represents the migration of legacy systems and interim systems to a Target System over time with milestones, migration, and sunset dates.

(1) Describe overall migration strategy (plans/milestones/sunset) for all Domain Target IT systems.

(2) Provide the Domain's current portfolio of IT investments currently underway, but not yet in use.



Domain PfM
Transformation Schedule (Fishbone)

Program Level:
Primary BEP:
Certification Authority:
Lead CBM:
Component:

FY03 FY04 FY05 FY06 FY07 FY08 FY09 FY10

Legacy System 1
Legacy System 2
Legacy System 3
Legacy System 4
Legacy System 5
10/2005 – 07/2008
Inc.1.3 Milestone C 07/01/2008
Inc. 1.2 IOC 12/01/2007
Inc. 1.2 Milestone B 01/01/2007
Inc. 2.0 Milestone C 03/31/2009
AoA 10/05/2004
Target System
Inc. 1.1 Milestone A 05/01/2005
Inc. 2.0 Milestone B 09/2008
FDDR 2 05/2009
FOC Inc. 2.0 FY 10
FDDR 1 10/2008
Interim System 1
2008
Interim System 2
TBD
10/2007 – 7/2008
Legacy System 6
Interim System 3
2008
Legacy System 7
Legacy System 8
2009
Legacy System 9
10/2009
Legacy System 10
TBD

12/2/2005
9

Figure B.8 – Domain PfM Transformation Schedule

B-9. Domain Portfolio System Review Dashboard

(Use template provided in Figure B.9 below)

a. The Domain Portfolio System Review Dashboard is required for all initiatives, systems and capabilities with Development / Modernization funding of > $1M and Sustainment funding of > $10M over the FYDP.

(1) Identify System Name.

(2) Identify Cost Level:

(a) Level 1 –Modernizations / sustainment greater than $32M

(b) Level 2 – Modernizations / sustainment of $10M up to $32M

(c) Level 3 – Modernizations / sustainment greater than $1M but less than $10M

(d) Level 4 – Modernizations / sustainment less than or equal to $1M

(3) Determine:

(a) Transition Plan State (Core, Interim or Legacy)

(b) PEG, MDEP, and Army Program Element (APE)

(c) Acquisition Category (ACAT I, ACAT IA, ACAT II or ACAT III)

(d) Mission Area and Domain Lead and Partner OSD IRB(s)

(e) If it is a Joint Initiative

(f) Dates of Last and Next Milestones

(g) Registry numbers in AITR, Selective and Native Programming Data Collection System – Information Technology (SNAP-IT) / Information Technology Management Application (ITMA) and DITPR

(4) Provide a summary description of the system.

(5) List three major capability gaps addressed by the system.

(6) Provide status of CTSF Integration / Interoperability Testing for this system.

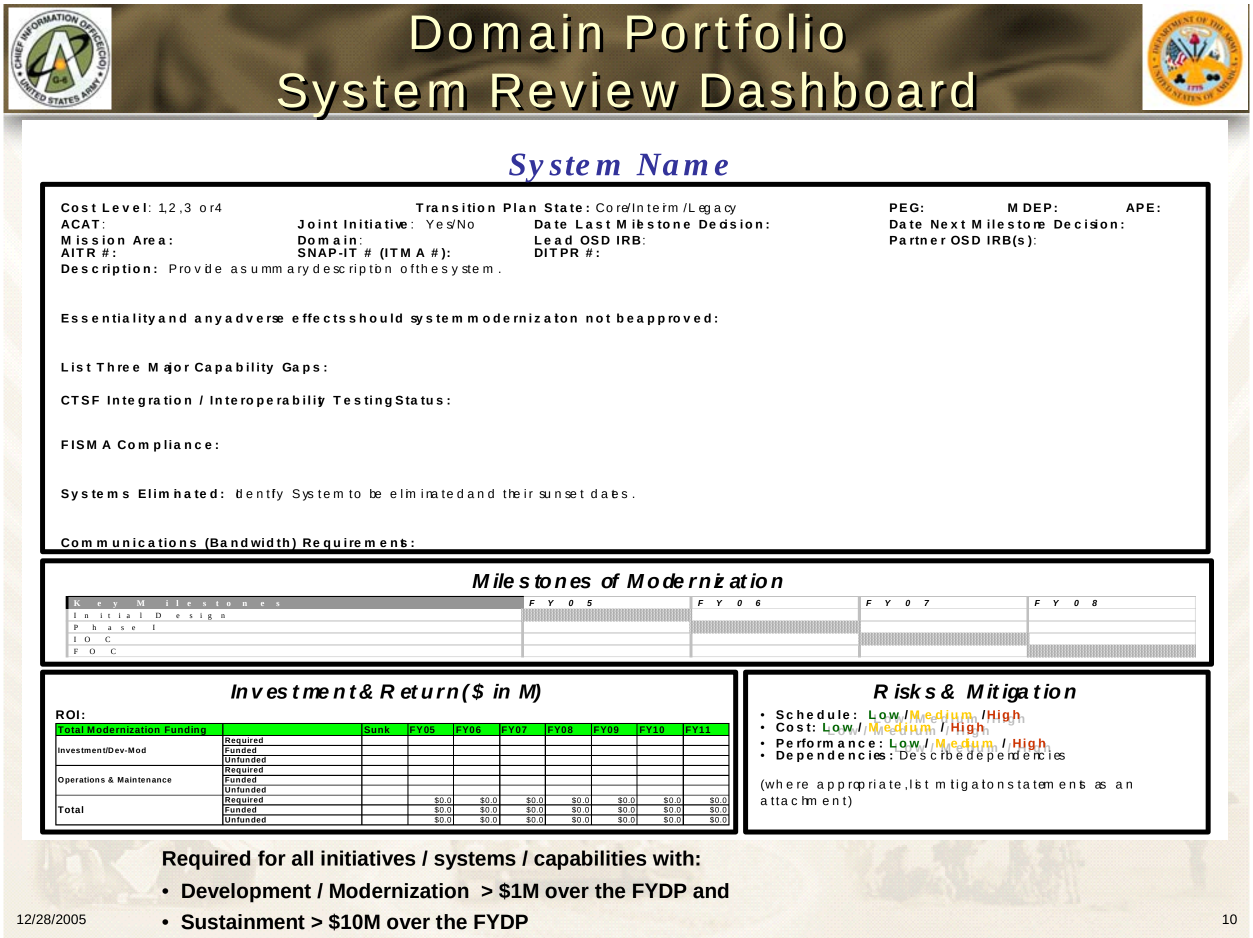
(7) Provide status of FISMA Compliance for this system.

(8) Identify Systems to be eliminated and their sunset dates

(9) Identify Milestones by Fiscal Year

(10) Complete Investment & Return by funding type: Dev/Mod and Operations & Maintenance (Required, Funded, Unfunded)

(11) Complete Risk & Mitigation using the Risk Definitions (see Figure B.10) for Schedule, Cost, Performance, and Dependencies.



Domain Portfolio System Review Dashboard

System Name

Cost Level: 1,2,3 or4 **Transition Plan State:** Core/Interim/Legacy **PEG:** **MDEP:** **APE:**

ACAT: **Joint Initiative**: Yes/No **Date Last Milestone Decision:** **Date Next Milestone Decision:**

Mission Area: **Domain**: **Lead OSD IRB**: **Partner OSD IRB(s)**:

AITR #: **SNAP-IT # (ITMA #):** **DITPR #:**

Description: Provide asummarydescription ofthesystem.

Essentialityand anyadverse effectsshould systemmodernizaton not beapproved:

List Three Major Capability Gaps:

CTSF Integration / Interoperabiliy TestingStatus:

FISMA Compliance:

Systems Eliminated: Identfy System to be eliminatedand their sunset dates.

Communications (Bandwidth) Requirements:

Milestones of Modernization

Key Milestones	FY05	FY06	FY07	FY08
Initial Design	▨			
Phase I		▨		
IOC			▨	
FOC				▨

Investment& Return($ in M)

ROI:

Total Modernization Funding		Sunk	FY05	FY06	FY07	FY08	FY09	FY10	FY11
Investment/Dev-Mod	Required								
	Funded								
	Unfunded								
Operations & Maintenance	Required								
	Funded								
	Unfunded								
Total	Required		$0.0	$0.0	$0.0	$0.0	$0.0	$0.0	$0.0
	Funded		$0.0	$0.0	$0.0	$0.0	$0.0	$0.0	$0.0
	Unfunded		$0.0	$0.0	$0.0	$0.0	$0.0	$0.0	$0.0

Risks & Mitigation

- **Schedule:** Low/Medium /High
- **Cost:** Low/ Medium /High
- **Performance:** Low/ Medium / High
- **Dependencies:** Describedependencies

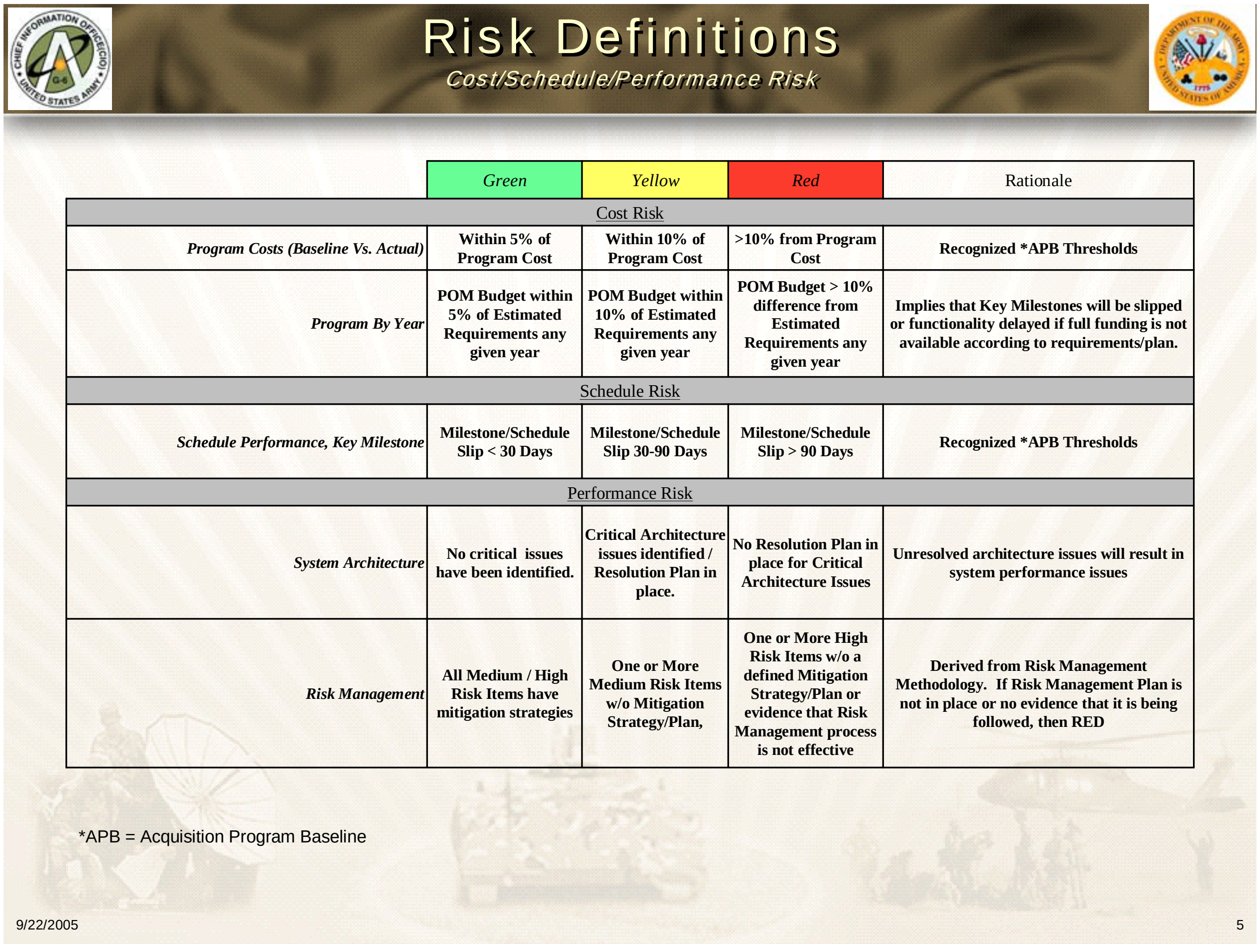
(where appropriate,list mitigatonstatements as an attachment)

Required for all initiatives / systems / capabilities with:

- **Development / Modernization > $1M over the FYDP and**
- **Sustainment > $10M over the FYDP**

12/28/2005 10

Figure B.9 – Domain Portfolio System Review Dashboard



Risk Definitions

Cost/Schedule/Performance Risk

	Green	*Yellow*	*Red*	Rationale
Cost Risk				
Program Costs (Baseline Vs. Actual)	**Within 5% of Program Cost**	**Within 10% of Program Cost**	**>10% from Program Cost**	**Recognized *APB Thresholds**
Program By Year	**POM Budget within 5% of Estimated Requirements any given year**	**POM Budget within 10% of Estimated Requirements any given year**	**POM Budget > 10% difference from Estimated Requirements any given year**	**Implies that Key Milestones will be slipped or functionality delayed if full funding is not available according to requirements/plan.**
Schedule Risk				
Schedule Performance, Key Milestone	**Milestone/Schedule Slip < 30 Days**	**Milestone/Schedule Slip 30-90 Days**	**Milestone/Schedule Slip > 90 Days**	**Recognized *APB Thresholds**
Performance Risk				
System Architecture	**No critical issues have been identified.**	**Critical Architecture issues identified / Resolution Plan in place.**	**No Resolution Plan in place for Critical Architecture Issues**	**Unresolved architecture issues will result in system performance issues**
Risk Management	**All Medium / High Risk Items have mitigation strategies**	**One or More Medium Risk Items w/o Mitigation Strategy/Plan,**	**One or More High Risk Items w/o a defined Mitigation Strategy/Plan or evidence that Risk Management process is not effective**	**Derived from Risk Management Methodology. If Risk Management Plan is not in place or no evidence that it is being followed, then RED**

*APB = Acquisition Program Baseline

9/22/2005

5

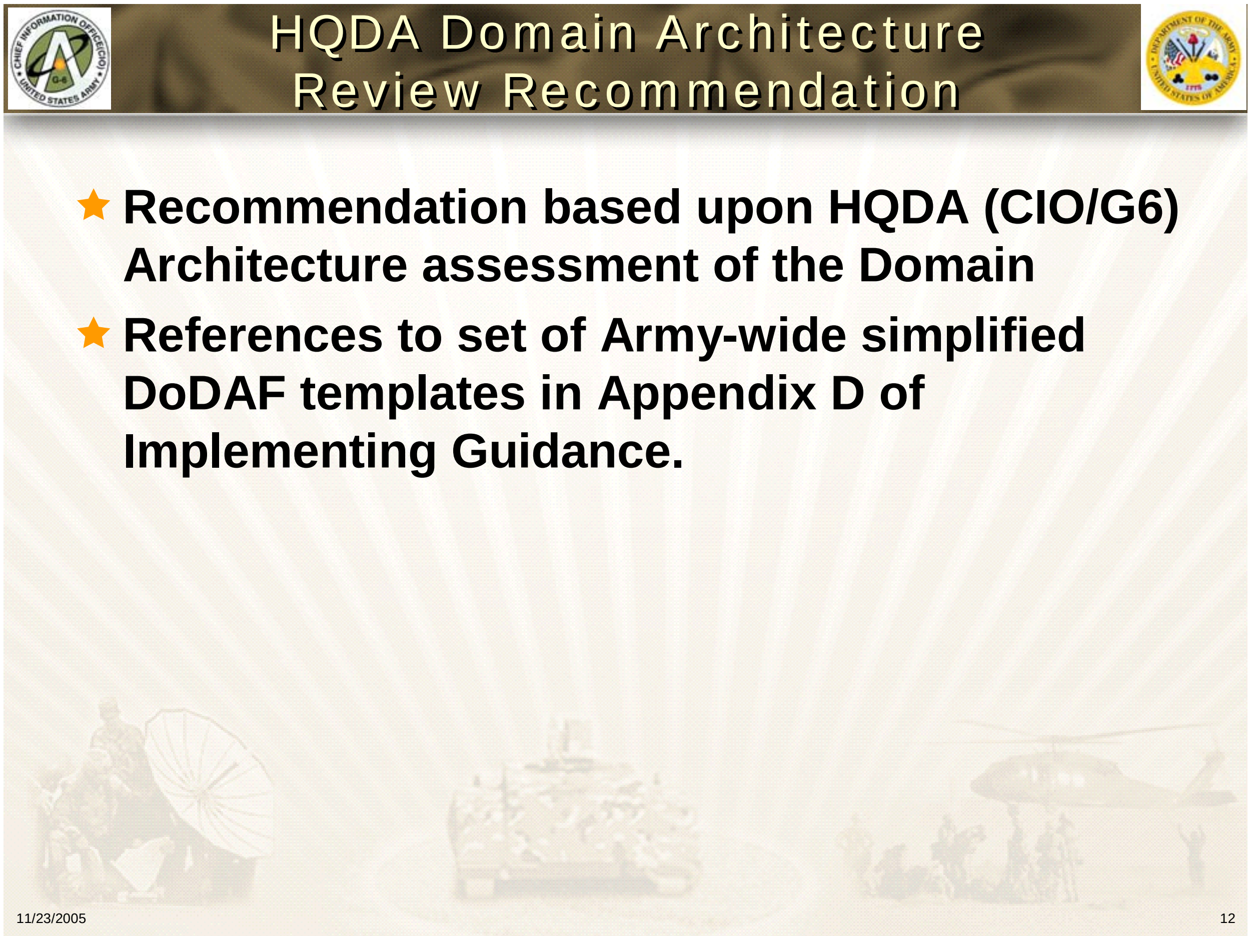
Figure B.10 – Risk Definitions

B-10. HQDA Domain Architecture Review Recommendation

(Use template provided in Figure B.11 below)

a. Recommendation based upon HQDA Architecture Assessment of the Domain.

b. References to set of Army-wide simplified DoDAF templates in Appendix C of Implementing Guidance.



HQDA Domain Architecture Review Recommendation

- Recommendation based upon HQDA (CIO/G6) Architecture assessment of the Domain
- References to set of Army-wide simplified DoDAF templates in Appendix D of Implementing Guidance.

11/23/2005

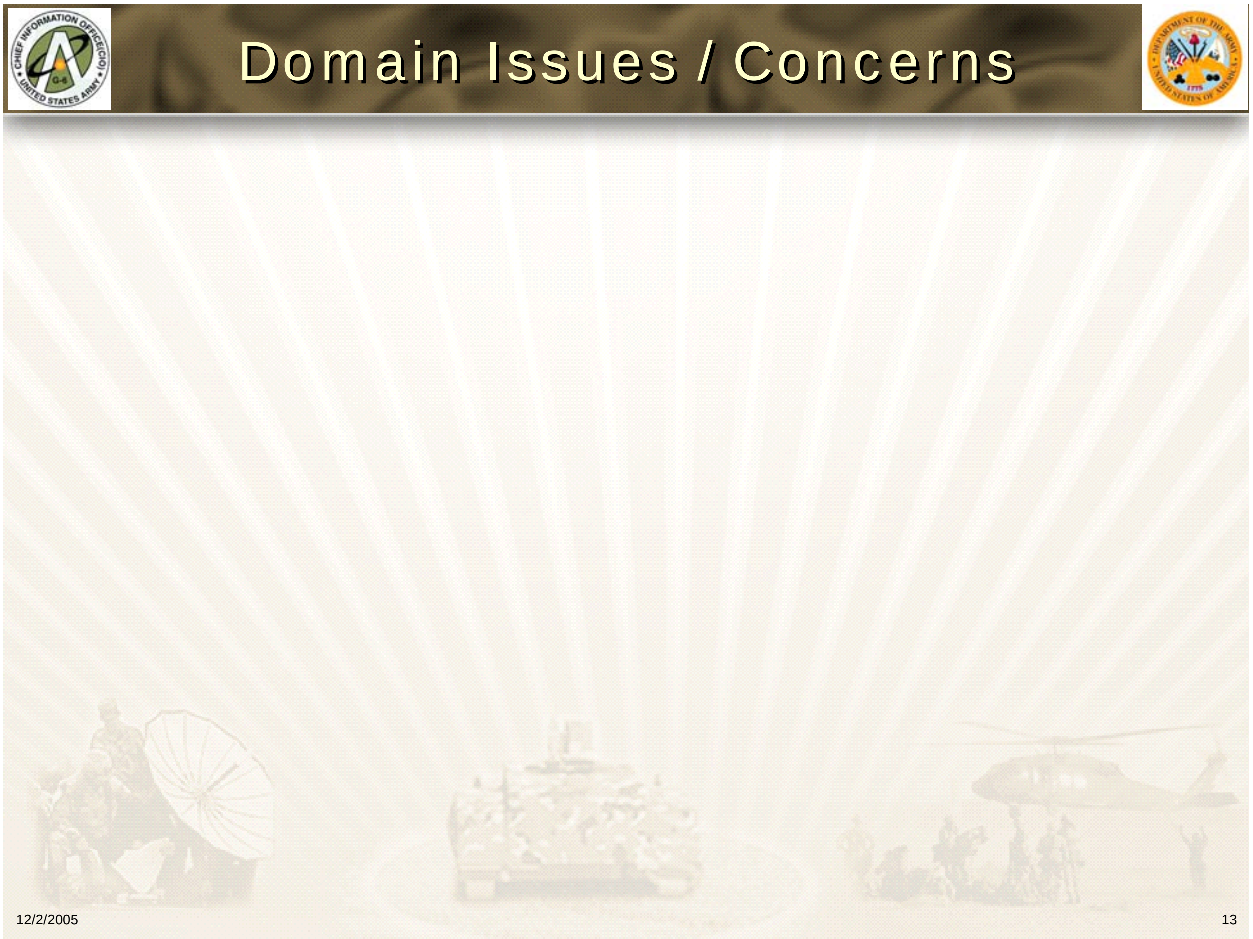
12

Figure B.11 – HQDA Domain Architecture Review Recommendation

B-11. Domain Issues/Concerns

(Use template provided in Figure B.12 below)

a. Provide any issues/concerns (i.e. Cross-MA issues, etc.).



Domain Issues / Concerns

12/2/2005

13

Figure B.12 – Domain Issues/Concerns

B-12. Domain Way-Ahead

(Use template provided in Figure B.13 below)

a. Provide Domain way-ahead (i.e. plans for interoperability, strategy for 80% goal, transformation schedule, etc.)

Domain Way Ahead

12/2/2005

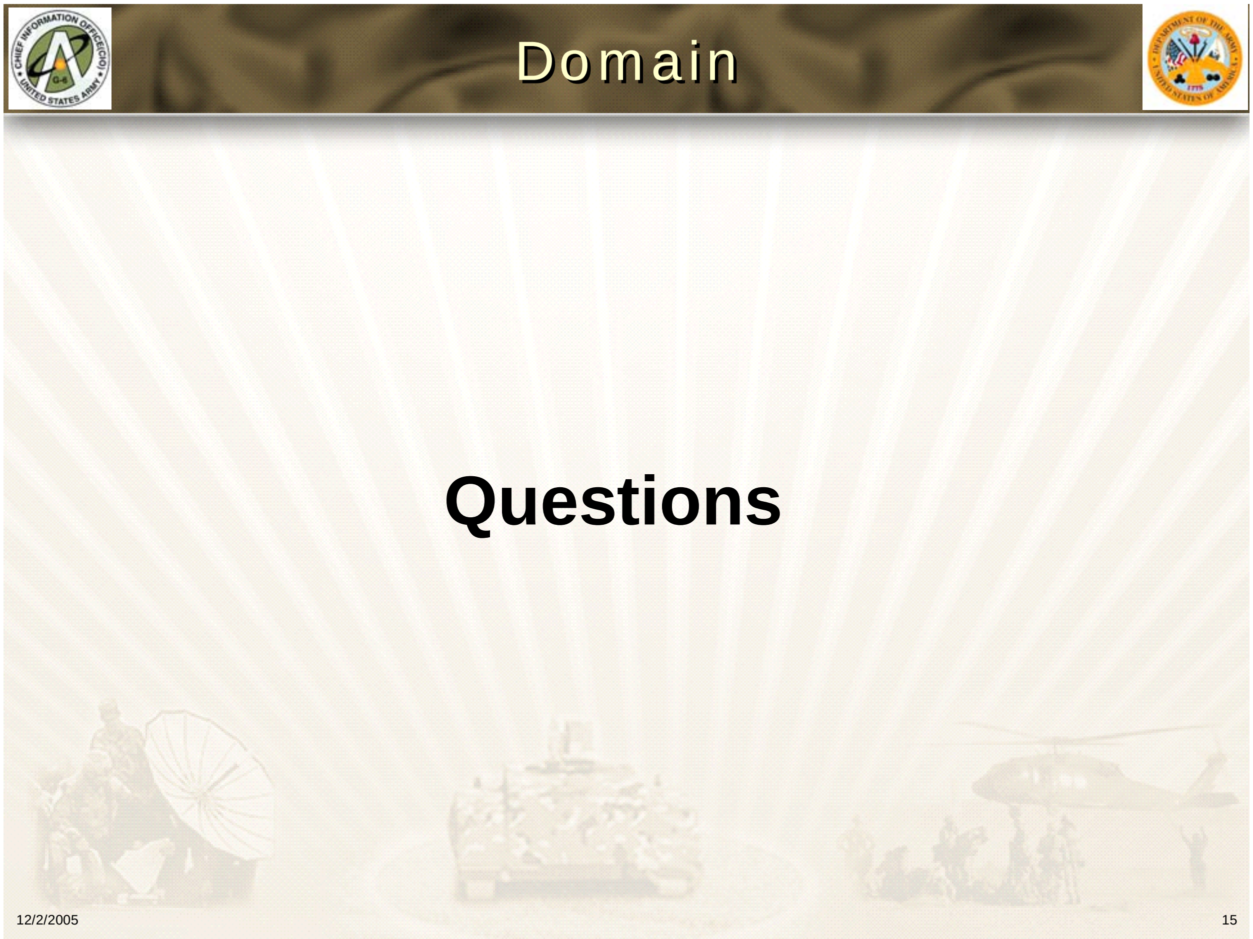
14

Figure B.13 – Domain Way-Ahead

B-13. Questions

(Use template provided in Figure B.14 below)

a. Q & A session / further discussion if needed.



Domain

Questions

12/2/2005

15

Figure B.14 – Mission Area Backups

B-14. Mission Area Backups

(Use template provided in Figure B.15 below)

a. Mission Area to provide any additional backup slides.

Mission Area

Back Ups

12/2/2005

16

Figure B.15 – Mission Area Backups

Appendix C
IT PfM Metrics And Performance Measurement

C-1. Army IT PfM Metrics and Performance Measurement

The Army will also employ Lean / Six Sigma and other industry best practices successfully used by the world's best corporations to provide better value to our increasing responsiveness and decreasing cycle time in all processes and activities. The Army is deploying these same techniques to better identify functions that are no longer relevant, to eliminate non-value added operations and positions, and to focus resources on our required capabilities. This is a transformational process that is being led from the highest levels of the Army.

C-2. Guidance for Development of Army IT PfM Performance Measures

a. The Army Balanced Scorecard is the metrics focal point for Strategic Readiness System (SRS). The Army Scorecard identifies the metrics -- quantifiable success measurements -- of each readiness area. Those areas are tied to the annual Army Campaign Plan (ACP) and the Army Posture Statement (APS) which include: status of the industrial base for military equipment and supplies, Well-Being, infrastructure of all Army installations and status of federal, state and local transportation nodes in reference to their abilities to support deployments.

b. Figure C.1 below depicts the Army use of the Balanced Scorecard methodology to communicate and align the Army's mission, vision, strategic objectives and priorities. The SRS captures information on the key elements/ends of the Army Transformation to include installations, infrastructure, Well-Being, the nation's industrial base, sustainment, and readiness. The Army is in the process of applying the SRS to the Army Transformation to measure progress.

c. CIO/G-6 is currently using the following performance measures for the SRS requirements:

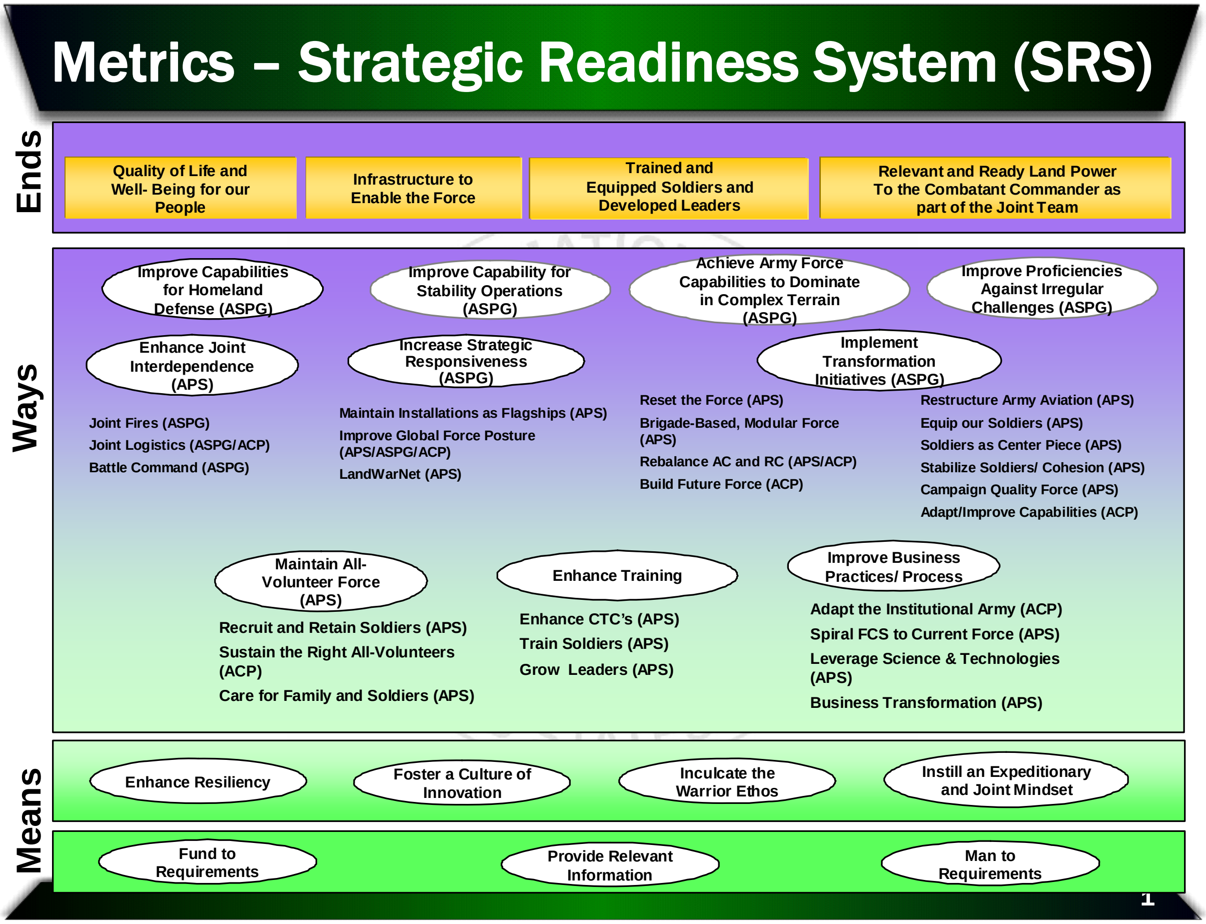
(1) % Reduction of redundant Army IT systems capabilities.

(2) Alignment of APMS-AITR systems to the Army’s Business Processes as deconflicted by the governing Domains.

(3) % of Mission Area / Domain IT Portfolio Reviews conducted

(4) Certification FY06 (e.g. BMMP and any future DoD required Certifications)

d. MAs and Domains are expected to develop their own metrics and performance measures to track and report key elements of their PfM / transformation activities and track them using the SRS.



Metrics – Strategic Readiness System (SRS)

Ends

Quality of Life and Well- Being for our People

Infrastructure to Enable the Force

Trained and Equipped Soldiers and Developed Leaders

Relevant and Ready Land Power To the Combatant Commander as part of the Joint Team

Ways

Improve Capabilities for Homeland Defense (ASPG)

Improve Capability for Stability Operations (ASPG)

Achieve Army Force Capabilities to Dominate in Complex Terrain (ASPG)

Improve Proficiencies Against Irregular Challenges (ASPG)

Enhance Joint Interdependence (APS)

Increase Strategic Responsiveness (ASPG)

Implement Transformation Initiatives (ASPG)

Joint Fires (ASPG)
Joint Logistics (ASPG/ACP)
Battle Command (ASPG)

Maintain Installations as Flagships (APS)
Improve Global Force Posture (APS/ASPG/ACP)
LandWarNet (APS)

Reset the Force (APS)
Brigade-Based, Modular Force (APS)
Rebalance AC and RC (APS/ACP)
Build Future Force (ACP)

Restructure Army Aviation (APS)
Equip our Soldiers (APS)
Soldiers as Center Piece (APS)
Stabilize Soldiers/ Cohesion (APS)
Campaign Quality Force (APS)
Adapt/Improve Capabilities (ACP)

Maintain All-Volunteer Force (APS)

Enhance Training

Improve Business Practices/ Process

Recruit and Retain Soldiers (APS)
Sustain the Right All-Volunteers (ACP)
Care for Family and Soldiers (APS)

Enhance CTC's (APS)
Train Soldiers (APS)
Grow Leaders (APS)

Adapt the Institutional Army (ACP)
Spiral FCS to Current Force (APS)
Leverage Science & Technologies (APS)
Business Transformation (APS)

Means

Enhance Resiliency

Foster a Culture of Innovation

Inculcate the Warrior Ethos

Instill an Expeditionary and Joint Mindset

Fund to Requirements

Provide Relevant Information

Man to Requirements

Figure C.1 - Metrics - Strategic Readiness System (SRS)

C-3. Categorized Examples of Performance Measures

The following table provides some examples of basic performance measures that could be used in managing the Army IT portfolios. Some are specific to IT PfM, and some are typical for many IT projects and activities. While the Category and Metrics columns are fairly representative of those used in IT projects in general, the Measures of Success will vary greatly and should be established and tailored for each individual MA and Domain PfM / transformation initiative and objective, as appropriate.

(Draft – Some Basic Performance Measures for IT Activities)

Category	Metrics	Purpose	Measure of Success
Compliance	Number of Mission Area /Domain IT Systems Identified as Core / Interim / Legacy and Base-lined in APMS-AITR module	Establish a complete inventory of Army IT systems to baseline Army IT investments	100% of known Army IT systems are in APMS-AITR module
	Number of Mission Area /Domain IT Capabilities Identified aligned to the system baseline above and Base-lined in APMS-AITR module	Establish a complete inventory of Army capabilities to improve Army IT investments	100% of known Army capabilities are in APMS-AITR module
	Number of Mission Critical / Mission Essential capability gaps identified	Provide Mission Critical / Mission Essential capabilities to meet Warfighter requirements	Reduced number of Mission Critical / Mission Essential capability gaps
	Number of systems compliant with CTSF Interoperability requirements.	Track progress towards system CTSF interoperability certification.	% of systems as Interoperable
	Number of MA/Domain IT Portfolio Reviews conducted	Track progress towards completion of reviews.	% of MA/Domain IT Portfolio Reviews conducted
	Number of systems requiring certification	Track progress towards certification of systems.	% of Certification FY06 (> $1M Development / Modernization)
	Number of Domains that have AEA aligned architecture	Track progress towards alignment to AEA	% of Domains that have an AEA aligned architecture.
Redundancy	Elimination of duplicate or overlapping Army systems.	Ensure return on investment.	% Retirement of identified duplicate systems
	Decreased number of duplicate data elements.	Reduce input redundancy and increase data integrity.	Data elements are entered once and stored in one database.
	Number of Mission Area/Domain redundant IT investments / capabilities / systems eliminated.	Make available scarce IT resources for higher priority investments / capabilities	80% reduction of duplicate IT investments / capabilities by EOFY 2007

Appendix D
Enterprise Architecture's (EA) Role in Portfolio Management

D-1. Background

a. Architectures must be considered when making IT investment decisions. Within DoD, high-level strategy and guidance statements (e.g., National Security Strategy (NSS), National Military Strategy (NMS), Joint Operational Concept (JopsC), Defense Planning Guidance (DPG), Unified Command Plans (UCP)) and overarching concepts statements establish the enterprise architecture. The IT enterprise architecture is defined in the Global Information Grid (GIG) Architecture, Net-Centric Operations and Warfare Reference Model (NCOW–RM), DoD Data Strategy, DoD Information Assurance (IA) Strategy, DoD Net-Centric (NC) Services Strategy, and other related guidance. MA/Domain Leads must ensure the development and utilization of MA/Domain architectures to include applicable IT systems/initiatives architectures are consistent with enterprise architecture requirements. Architecture products provide an essential tool for effectively and efficiently engineering operational processes and information exchanges, and for implementing and evolving supporting systems.

b. An MA/Domain Enterprise Architecture is a description of the MA/Domain including organizational stakeholders, high level capability requirements, process flows and supporting infrastructure. A complete MA/Domain Enterprise Architecture includes both an "as-is" (current) description and a "to-be" (future) description of the enterprise, in support of MA/Domain transformation plans for migrating from the as-is to the to-be (which may include transitional architectures).

c. The Army Enterprise Architecture (AEA) is a federated architecture which brings together all of the MA and Domain Enterprise Architectures which are inherently a part of the Army Enterprise. The AEA will align to Federal, Joint and DoD Architectures.

D-2. Objective

a. In support of Portfolio Management, the enterprise architectures provide information required to drive the following initiatives:

(1) Drive all Army systems to be developed as modular, joint and interoperable;

(2) Expedite the fielding of Army systems by providing enhanced requirements documentation and meeting all statutory, regulatory and policy requirements with respect to architecture development and compliance; and

(3) Harmonize touch-points, between and amongst disparate/federated architectures and work to identify and reduce capability gaps and overlaps.

(4) Drive interoperability and integration of capabilities

(5) Create robust baselines of portfolios of processes, programs, systems and outcomes,

(6) Perform an integrated analysis of gaps and opportunities, using robust methodologies, common assumptions, and advanced analytical tools,

(7) Establish approaches that lead to integrated materiel and non-materiel solutions

(8) Promote the Net-Centric data strategy to enable data interoperability

D-3. HQDA Architecture Roles in PfM

a. G-3/5/7

(1) The G-3/5/7 is the Chief Architect of the Army.

b. CIO/G-6

(1) To support this effort across the Army, the HQDA CIO/G-6 will establish an EA Support Team within the Army Architecture and Integration Cell (AAIC). This team will work in coordination with ASA(AL&T), HQDA G-3/5/7 and Training & Doctrine Command (TRADOC) to serve as an Army enterprise level asset to support all Army MA and Domain Leads and members in the development and use of their architecture products.

(2) Specifically, in support of MA and Domain Leads, the CIO/G6 EA Support Team will:

(a) Establish and co-chair (with ASA(AL&T) and TRADOC) a collaborative working group called the Enterprise Architecture Working Group (EAWG). This group will develop common architecture tools and templates all Army MAs and Domains will use in order to standardize architecture integration efforts across the Army.

(i) Ensure that the Army templates are aligned to existing DoD Architecture Framework (DODAF) views.

(b) In coordination with the EAWG, ASA(AL&T) and TRADOC, the CIO/G-6 will publish revised templates annually with a prescribed list of the minimum basic artifacts to fully depict an enterprise architecture at the MA and Domain levels.

(i) The required list of standard templates published by CIO/G6 will be used and submitted by every Army MA and Domain in the following Fiscal Year for validation and inclusion in the Federated AEA.

(ii) The CIO/G-6 will publish each year's templates no later than 30 JUNE of the previous year to allow Domains time to plan and budget the following year's architecture development activities accordingly.

(c) The CIO/G-6 will provide technical advice and guidance to MA and Domain Leads, including the maintenance of an EA Community Forum in AKO with standardized Army architecture templates, examples and easy to follow instructions for the development of architecture products.

(d) The CIO/G-6 will federate/integrate Army MA and Domain Architecture products, maintaining a central repository and publishing (annually) the federated AEA.

D-4. Mission Area Lead Actions

a. Coordinate with JCS/OSD Mission Area counterparts as appropriate

b. With the Army architects, ensure development of the following Architecture products using formats and tools provided by CIO/G-6:

(1) A view which shows the assignment of capabilities to Domains within the MA

(2) A view which identifies the major stakeholders within the MA

c. MAs must develop and maintain architecture products prior to the MA review.

d. MA will review Domain Architecture products.

e. Ensure that the development of MA Architecture products is the documentation of the results of a concerted strategic and technical planning effort that starts with forward looking operational needs assessments and ends with the identification of an infrastructure design that optimizes available resources to meet the requirements of the enterprise.

f. Each Army MA Lead will, at a minimum:

(1) Provide a representative to participate in the EAWG;

(2) Harmonize cross-MA/Domain information exchange standards;

(3) Approve Domain Architecture products within their MA; and

(4) Make iterative improvements in their MA architecture products as required in accordance with the architecture validation and publication process described below.

D-5. Domain Lead Actions

a. Coordinate with MA Leads as appropriate.

b. With the Army architects, ensure development of the following Architecture products using formats and tools provided by CIO/G-6:

- A view which provides a common capabilities taxonomy for the domain which is used by all programs/initiatives within the Domain to identify and map their capabilities
- A view which identifies all inter-Domain interoperability touchpoints and capability gaps and overlaps between systems
- A view which identifies all intra-Domain interoperability touchpoints and capability gaps and overlaps between systems
- A view which identifies all bandwidth requirements for Domain systems across the enterprise
- A view which identifies all the technical and information standards which systems within the Domain must comply with and/or use

c. Domain leaders will validate that all IT investments are aligned with Army operational capabilities

d. Ensure that the development of Domain architecture products is the documentation of the results of a concerted strategic and technical planning effort that starts with forward looking operational needs assessments and ends with the identification of an infrastructure design that optimizes available resources to meet the requirements of the enterprise.

e. Domain Leads will:

(1) Provide a representative to participate in the EAWG;

(2) Harmonize internal Domain information exchange standards;

(3) Submit their Domain Architecture products for approval to the appropriate MA Lead and, in coordination with CIO/G-6, have Domain architecture products validated and published;

(4) Make iterative improvements in their Domain Architecture products as required in accordance with the architecture validation and publication process described below.

D-6. Architecture Validation and Publication Process

a. Army Domain Architecture products will be submitted and validated annually to ensure valid and current architectures are available to support milestone decisions, portfolio reviews, and other leadership decisions. The validation process will not look at capabilities, systems and processes that sit wholly within a Domain but rather would focus on touch points and intersections where mission threads cross Domains and have impacts outside of that Domain and where capability gaps and overlaps exist across Domains.

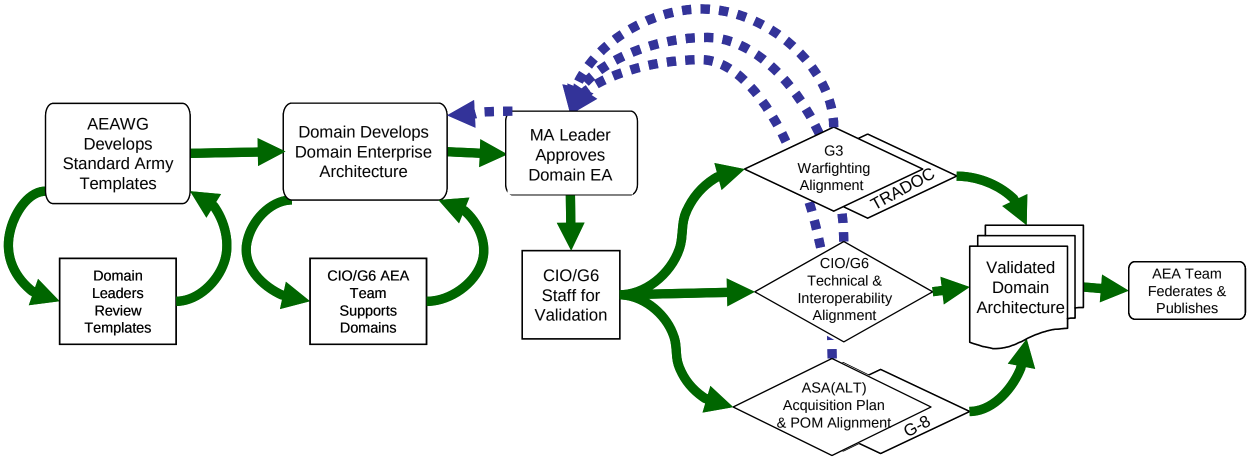

AEAWG Develops Standard Army Templates
Domain Leaders Review Templates
Domain Develops Domain Enterprise Architecture
CIO/G6 AEA Team Supports Domains
MA Leader Approves Domain EA
CIO/G6 Staff for Validation
G3 Warfighting Alignment
TRADOC
CIO/G6 Technical & Interoperability Alignment
ASA(ALT) Acquisition Plan & POM Alignment
G-8
Validated Domain Architecture
AEA Team Federates & Publishes

Figure D-1 Architecture Validation and Publication Process

b. The purpose of the validation process is not to second guess business processes or functional requirements developed and approved by MA and Domain Leads, but rather to ensure alignment across MAs and Domains. The validation process will ensure that Domain Architecture products:

(1) Meet operational needs, capability requirements and priorities of the Army;

(2) Align to, and federate with, other Army, Joint or DoD Level Architectures and guidance (e.g., DoD Information Technology Standards Registry (DISR), DoD-BEA, Army Software (SW) Blocking, NCOW-RM, etc.); and

(3) Align to Army and DoD transformation and modernization initiatives if applicable.

D-7. Architecture Support for Portfolio Management (PfM)

a. Army is implementing a two-phased process for architecture validation in support of PfM and other decision making processes. Gaining approval of Domain Architecture products in advance, decreases architecture submission requirements for individual programs and expedite portfolio reviews. This process will also serve to expedite Milestone Decision, Operational Needs Statement Authority and other decision and certification package routing and approvals.

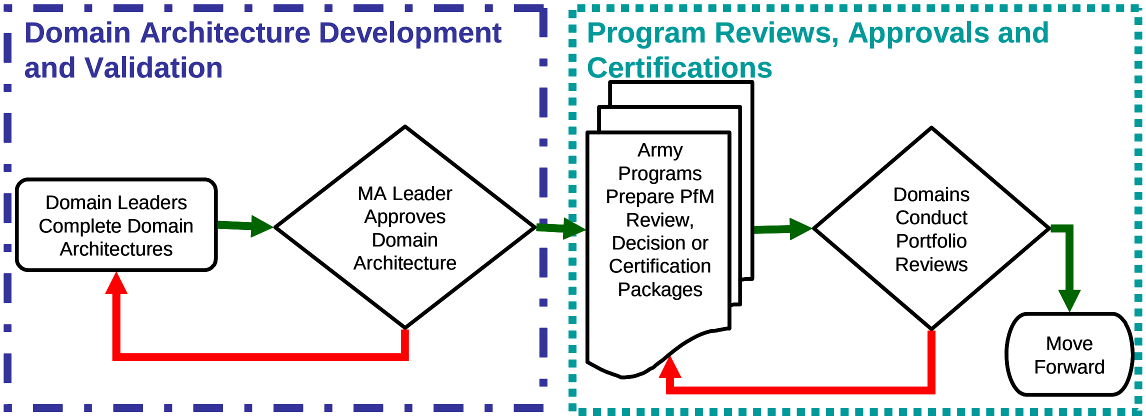

Domain Architecture Development and Validation
Domain Leaders Complete Domain Architectures
MA Leader Approves Domain Architecture
Program Reviews, Approvals and Certifications
Army Programs Prepare PfM Review, Decision or Certification Packages
Domains Conduct Portfolio Reviews
Move Forward

Figure D-2 – Army "Two-Step" Process

b. This two-step process will fulfill Army requirements and enable full compliance with appropriate laws and regulations. Using this system, architecture validation and certification staffs will be able to focus on approval of Architectures, and thereby minimize the time and effort required to validate/certify individual programs. Moreover, this two step process will drive the Army down a path toward documenting architectures in a manner that actually makes them usable as executive management tools.

Appendix E
Army Portfolio Management Solution (APMS) - Portfolio Management Decision Support Tool

a. As the CIO/G-6 worked to develop an integrated IT PfM governance structure within the DoD direction and guidance to meet the responsibilities directed in the Clinger-Cohen Act, it was recognized that a PfM Decision Support Tool is required to enable true enterprise PfM. A detailed process was undertaken within CIO/G-6 reviewing and evaluating potential GOTS and COTS products that had the potential to meet the need.

b. The APMS Decision Support Tool uses the COTS tool as the base, configured to meet the Army unique requirements. APMS met or exceeded all evaluative criteria used during the tool selection process, and will be configured with modules to support the separate, but related and integrated, pieces of PfM. The initial implementation of APMS allowed for the distribution of 5,000 licenses across the Army ensuring all required individuals who support the Army governance processes have access to and are trained in the use of the system. MACOMs and Commands are capable of extending the current configuration of the tool to support their unique needs, as long as all extensions are coordinated through the APMS Configuration Control Board (CCB). The APMS CCBs will be held on a quarterly basis with the first held in the 1st Quarter FY06.

c. During the Evaluation Phase, the requirements for any PfM tool included the capability to:

(1) Facilitate data collection with Web-based forms and supports all common data types. Use an open architecture and standard database configurations to upload data from other systems, thereby leveraging, not replacing, existing databases. Data security must be developed to meet DoD standards. This system will record and display transaction information.

(2) Utilize wizards and a broad range of configurable fields encompassing all data type and calculations required for process support. Possess an internal query-based analytical capability that would support multidimensional views to integrate budget and performance information. Enable linkage and tracking of actions items, documents, dependencies and resources to the investment.

(3) Support the Select Phase with forms to collect data, scorecards with calculated values (ROI, NPV, etc) to review information and multidimensional maps to evaluate alignment, balance, priority, performance and cost of IT investments. Enables Capital Planning & Investment Control (CPIC) budgeting processes needed for submission of Exhibits 300 and 53 to OMB, including automated optimization to facilitate “pass back” funding decisions. Permit creation, monitoring and distribution of standard lifecycles across the enterprise.

(4) Support the Control Phase with forms to collect data, scorecards with calculated values (capability acquisition, milestone/deliverable completion, EVM, risk, etc) to review information and multidimensional maps to facilitate visualization of a large number of investments and management by exception. All views need to be re-usable and re-configurable. Enable full lifecycle monitoring and provide a configuration for the Federal Enterprise Architecture (FEA).

(5) Support the Evaluation Phase with post-implementation reviews, assessments, what-if planning/scenarios and other performance indicators.

(6) Support many to many relationship between IT investments and portfolios, allowing the same investment to reside in multiple portfolios. Provide unlimited flexibility in creating portfolios based on business need or analytic requirements

(7) Provide cross-Domain and cross-MA/Enterprise insights into proposed IT investments in support of strategic decision making

(8) Allow on-line collaboration while viewing portfolio data; enables knowledge management; different access levels in relation to user level

d. The final evaluation and selection of the COTS product to support the IT PfM requirement was made in coordination between the Army CIO/G-6 and the Assistant Secretary of the Army (Financial Management and Comptroller) (ASA(FM&C)), who directed the tool be developed to: meet the requirements for registration and reporting of IT Investments; meet the emerging Domain Certification requirements; support cross-MA and Domain analysis of IT investments to identify duplicate, redundant or inefficient investments where expended dollars could be recapitalized; and, support the development of the Army's IT Investment Strategy used during the Army budget process.

e. The APMS-Domain Certification (ADCM) module will support the preparation of the documentation necessary to support Domain level reviews of IT investments. Intense efforts will be made to rationalize any conflicts which may become evident as the DoD MAs mature and their processes become better defined. It is intended that the ADCM become the Army's repository for all Domain Certification packages submitted through Army to DoD. The ADCM module will also support Domain level reviews of investments they fund by capability, identifying within their Domain the 'best-practices' to be adopted and where strategic level decisions can be made regarding investments, thereby ensuring their investments best meet the needs within their Domain.

f. The APMS-Capital Planning and Investment Management (APMS-CPIM) module integrates the efforts achieved through the APMS-DC level and reviews/analyzes IT investments at the MA/Enterprise. All IT investments are reviewed by capabilities each provide and then evaluated using a set of analytical evaluative criteria. The analytical criteria include: Strategic Alignment; Capability Justification; Performance Outcome/Achievement; Functional Interdependencies; Mission Criticality; Integration and Risk; and Cost and Confidence. These categories serve as the basis for an evaluation of each proposed investment by Health, Risk and Value which can then be viewed through a series of pair-wise comparisons and investor maps. APMS-CPIM enables identification of duplicate or inefficient investments across the Enterprise, resulting in an IT Investment Strategy, prioritized by the funding Program Evaluation Group (PEG), to support the budget development.

g. The PfM registration and reporting requirement will be accomplished using the APMS-AITR module, which will subsume and replace the existing AITR system as the Army's IT Registry. This module will serve as the point from which all external IT registry reports are generated (i.e. DoD ITR reporting requirements), and is also the point where MACOMs/Commands register their existing IT investments, specifying the capability each provides and which MA/Domain they think the investment best aligns within. The APMS-AITR module will be the Army's IT repository of record.

E-1. APMS-AITR Module Criteria

a. The APMS-AITR module is the Army's single authoritative registry for Information Technology (IT) investments/capabilities/systems. The APMS-AITR module is used to manage the Mission Critical (MC), Mission Essential (ME), and Mission Support (MS) systems that are reported to the Office of the Secretary of Defense (OSD), Office of Management and Budget (OMB), and Congress. OSD also uses APMS-AITR module to compile and extract the Federal

Information Security Management Act (FISMA) Report, in accordance with the E-Government Act of 2002 (44 U.S.C. Chapter 36).

b. While Army MA/Domain Leads are responsible for managing IT capabilities as portfolios, MACOMs and system owners are responsible for certifying their Army Portfolio Management Solution (APMS)-Army Information Technology Registry (AITR) records as accurate and complete. Any system categorized as National Security System (NSS), or that has an Acquisition Category (ACAT) level or a Mission Assurance Category (MAC) level is, by definition, considered to be a "system" and shall be reported in the APMS-AITR module.

c. The following criteria are to be used to determine APMS-AITR system input eligibility:

(1) The Army is a funding source and/or primary manager (e.g., Executive Service of a Joint program, with the exception of Intel systems which are reported in the Defense Intelligence Mission Area); and

(2) The item is

(a) A system of systems; or

(b) A family of systems; or

(c) An information system; or

(d) An application; or

(e) A network; and

(3) The item is

(a) Funded at greater than $25,000 in any year of the Future Year Defense Program (FYDP) across all appropriations; or

(b) Commercial Off-The-Shelf (COTS) software with greater than $25,000 in customizations in any year of the FYDP; or

(c) An IT investment with at least one development/modernization task funded at more than $1M over all years of the FYDP; or sustainment over $10M; and

(d) Requires network access; and

(e) Accreditable Army Information System per the DITSCAP/DIACAP; and

(f) The item can be reported without divulging classified information.

d. Specific examples of Army items required to be included:

(1) Any Acquisition Category (ACAT) System;

(2) Any National Security System (NSS);

(3) Any Mission Assurance Category (MAC) System;

(4) Any Major Command (MACOM) Standard System;

(5) Any Below Major Command (MACOM) Systems (e.g., bridges, unique used at a single site, etc);

(6) Automated Information Systems (AIS);

(7) Data Stores (or Data Warehouse) – (i.e., a static, historical database, active, etc.);

(8) Portals; and

(9) Financial and "Mixed" Systems

e. Specific examples of items to be reported only as part of another reported system (i.e., not reported separately):

(1) Modules;

(2) Subsystems;

(3) Software Product/Suite;

(4) Information Technology (IT) Labor Skill;

(5) Internal script;

(6) Open Data-Base Connectivity Object;

(7) Portals associated with a specific, reported item; and

(8) Commercial-Off-The-Shelf (COTS) Office Automation

f. Specific examples identified below are excluded unless directly related to a system:

(1) An Information Assurance Initiative;

(2) An Architecture Initiative;

(3) Data Management Initiative;

(4) Intelligence Systems;

(5) Peripheral Equipment or Personal Digital Assistant (PDA); and

(6) A report

g. Computing Infrastructure components to be reported

(1) Peripheral Equipment or PDA not associated with a reported system

h. Steps to Add/Delete a System (The requirements for adding and the authority for deleting systems from the APMS-AITR module can be found at the URL https://apms.us.army.mil/).

(1) Show/Open the My Portfolios Bar (left hand side of window).

(2) Click on the Drop-down menu.

(3) Open the Executive Reviewers Operations folder; Open the Army Operational Processes sub-folder; Open the Army – Add a System folder; and Click on the Army Registration Request folder to view instructions in adding a system.

(4) Open the Executive Reviewers Operations folder; Open the Army Operational Processes sub-folder; Open the Army – Delete a System folder; and Click on the Army Deletion Request folder to view instructions in deleting a system.

(5) Another source for instructions in adding/deleting a system can be found in the APMS Fundamentals Training Manual (23 Nov 05) on the AKO APMS Community Page (URL https://www.us.army.mil/suite/page/84688).

Appendix F
Interoperability Testing, Certification and Configuration Management at the Central Technical Support Facility (CTSF)

a. Per the DoD Instruction 4630.8 Para 4, DoD policy requires that IT and NSS employed by U.S. Forces shall, where required (based on capability context), interoperate with existing and planned, systems and equipment, of joint, combined and coalition forces and with other U.S. Government Departments and Agencies, as appropriate. The Department of Defense shall achieve and maintain decision superiority for the warfighter and decision-maker by developing, acquiring, procuring, maintaining, and leveraging interoperable and supportable IT and NSS.

b. The CIO/G-6 is responsible to the SA and to the CSA to ensure IT and NSS are interoperable. To accomplish this task, the Central Technical Support Facility (CTSF) will execute the direction of the CIO/G-6 in support of this specific mission. Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA(ALT)) , in partnership with the CIO/G-6, will establish the support structure to execute this mission. This partnership will allow for the implementation of the necessary architecture, engineering and development required to support the prioritized capability as identified by the G-3/5/7 to support Warfighter specific requirements.

c. The CTSF is charged with rapidly developing, fielding and supporting leading-edge, secure and interoperable tactical, theater, and strategic command, control and communications systems. The facility offers systems interoperability, integration testing, configuration management and field engineering to Army Mission Areas and Domains.

d. The CTSF will serve as the single integrating point for Battle Command (BC) technical capabilities integration. The CIO/G-6 is responsible for ensuring necessary database, overall systems, and architecture modifications are implemented to achieve the greatest degree of technical integration and interoperability proficiency as rapidly as possible with the goal of meeting Commander's concerns as ABCS 6.4 is fielded across the Army.

e. MA and Domains will perform a review of all systems and report whether their systems are systems of record and submit them as appropriate for interoperability testing and "ruthless configuration management" at the CTSF. MA and Domains will ensure their IT Portfolio reviews identify and discuss systems/capabilities and their proposed schedule for interoperability and integration testing and configuration management at the Central Technical Support Facility (CTSF).

f. Intra-Army Interoperability Certification (IAIC) requires the following requirements:

(1) Any System that has a Requirement to be Interoperable with a Current Force System

(2) C4I Systems that have a Command, Control, Communications or Intelligence Function from Army Forces Down to Squad Level

(3) IAIC is Required for Each Version to be Released to the Field

(4) IAIC is not Army Battle Command System-Centric

(5) Any Army Business Systems that Interoperate with C4I Systems

(6) PMs Must Complete IAIC Prior to Acquisition Milestone C FRP or IPR

Current Force Systems – Those Systems Fielded Prior to December 2000- Must Certify All Hardware and Software Upgrades or Changes Prior to Fielding of Upgrade

Appendix G
Business Mission Area (BMA)

To be provided by the BMA – end of 3rd Quarter FY06

Refer to URL (TBD).

G-1. Governance

a. DoD

b. Army

c. Army Mission Area Alignment with DoD

G-2. MA IT Portfolio Management Process

G-3. Mission Area Enterprise Architecture Compliance

G-4. MA Plan/Timeline for Duplicate Capability Reduction by 2007

Appendix H
Warfighting Mission Area (WMA)

To be provided by the WMA – end of 3rd Quarter FY06.

Refer to URL (TBD).

H-1. Governance

a. DoD
b. Army
c. Army Mission Area Alignment with DoD

H-2. MA IT Portfolio Management Process

H-3. Mission Area Enterprise Architecture Compliance

H-4. MA Plan/Timeline for Duplicate Capability Reduction by 2007

Appendix I
Enterprise Information Environment Mission Area (EIEMA)

To be provided by the EIEMA – end of 3rd Quarter FY06.

Refer to URL (TBD).

I-1. Governance

a. DoD

b. Army

c. Army Mission Area Alignment with DoD

I-2. MA IT Portfolio Management Process

I-3. Mission Area Enterprise Architecture Compliance

I-4. MA Plan/Timeline for Duplicate Capability Reduction by 2007

Appendix J
Defense Intelligence Mission Area (DIMA)

To be provided by the DIMA – end of 3rd Quarter FY06.

Refer to URL (TBD).

J-1. Governance

a. DoD
b. Army
c. Army Mission Area Alignment with DoD

J-2. MA IT Portfolio Management Process

J-3. Mission Area Enterprise Architecture Compliance

J-4. MA Plan/Timeline for Duplicate Capability Reduction by 2007

Appendix K
References

Section I
Required Publications

AR 25-1
Army Knowledge Management and Information Technology, July 15, 2005.
(Available at http://www.army.mil/usapa/epubs/pdf/r25_1.pdf)

Army Net-Centric Data Management (ANCDM) Strategy (Draft)

Army Knowledge Management (AKM) Guidance Memorandum
Capabilities-Based Information Technology (IT) Portfolio Governance, July 20, 2005.

CJCS Memorandum
Assignment of Warfighting Mission Area (WMA) Responsibilities to Support Global Information Grid Enterprises Services (GIG ES), September 8, 2004.

DA Pam 25-1-1
Installation Information Services, August 27, 1991.
(Available at http://www.army.mil/usapa/epubs/pdf/p25_1_1.pdf)

DepSecDef Memorandum
Information Technology Portfolio Management, March 22, 2004.

Department of Defense Investment Review Process Overview
and Concept for Operations for Investment Review Boards May 17, 2005.

Department of Defense Net-Centric Data Strategy
May 9, 2003.

DoD CIO Memorandum
Enterprise Information Environment Mission Area (EIEMA) Domain Owner Designations, July 14, 2004.

DoD Enterprise Transition Plan
September 30, 2005.

DoDD 8000.1
Management of DoD Information Resources and Information Technology, February 27, 2002

DoDD 8100.1
Global Information Grid (GIG) Overarching Policy, September 19, 2002

DoDD 8115.01
Information Technology Portfolio Management, October 10, 2005.

DoDD 8320.2
Data Sharing in a Net-Centric Department of Defense, December 2, 2004.

DoDI 4630.8
Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), June 30, 2004.
(Available at http://www.dtic.mil/whs/directives/corres/xml/i46308x.xml)

DoDI 5000.2
Operation of the Defense Acquisition System, May 12, 2003.

DoDI 8115.bb
Draft Implementing Instructions to the DoD Information Technology Portfolio Management (DoD Directive 8115.01), November 3, 2005

HQDA General Order 2002-03
Assignment of Functions and Responsibilities within Headquarters, Department of the Army, July 9, 2002.

National Institute of Standards and Technology (NIST) Special Publication 800-59
Guideline for Identifying an Information System as a National Security System, August, 2003.

OMB Cir A-130
Management of Federal Information Resources, Revised, November 28, 2000.
(Available at http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html)

P.L. 104-106
Clinger-Cohen Act of 1996 (40 USC §§ 11312 & 11315)
(Available at http://www.gpoaccess.gov/plaws/index.html.)

The Ronald W. Reagan National Defense Authorization Act for Fiscal Year (FY) 2005, § 332
Defense Business Enterprise Architecture

SA Memorandum
Management Oversight of the Army's Business Transformation Initiatives, September 27, 2005.

Title X
United States Code

VCSA Memorandum
Global Information Grid Mission Area Roles, Responsibilities, and Development, October 8, 2004

Glossary

Section I
Abbreviations

AAA
Army Audit Agency

AAIC
Army Architecture Integration Cell

ACAT
Acquisition Category

AEA
Army Enterprise Architecture

AIS
Automated Information System

AITS
Automatic Intelligence Information Systems

AKO
Army Knowledge On-Line

APG
Army Planning Guidance

APMS
Army Portfolio Management Solution

ARSTAFF
Army Staff

ASA (AL&T)
Assistant Secretary of the Army (Acquisition, Logistics & Technology)

ASA (FM&C)
Assistant Secretary of the Army (Financial Management and Comptroller)

ASD (NII/CIO)
Assistant Secretary of Defense for Networks and Information Integration / CIO

AT&L
Acquisition, Technology & Logistics

ATO
Authority To Operate

AV
All View (DoDAF)

AV-1
Overview and Summary Information

AV-2
Integrated Dictionary

BEA
Business Enterprise Architecture

BMA
Business Mission Area

BMMP
Business Management Modernization Program

CA
Certification Authority

CBM
Core Business Mission

CCA
Clinger-Cohen Act

CDD
Capabilities Design (or Development) Document

CIO/G-6
Chief Information Officer/G-6

COI
Community of Interest

COTS
Commercial Off-The-Shelf

CPD
Capability Production Document

CPIC
Capital Planning and Investment Control

CPIM
Capital Planning and Investment Management

DAS
Defense Acquisition System

DBSMC
Defense Business System Management Committee

DEPSECDEF
Deputy Secretary of Defense

DIACAP
DoD Information Assurance Certification and Accreditation Process

DIMA
Defense Intelligence Mission Area

DITPR
DoD Information Technology Portfolio Repository

DITSCAP
DoD Information Technology Security Certification and Accreditation Process

DEV/MOD
Development/Modernization/Enhancement

DoD
Department of Defense

DoD EA RM
DoD Enterprise Architecture Reference Model

DoDAF
DoD Architecture Framework

DoDD
Department of Defense Directive

DRM
Data Reference Model

EA

Enterprise Architecture

E-Government
Electronic Government Act

EIEMA
Enterprise Information Environment Mission Area

ERP
Enterprise Resource Planning

ETP
Enterprise Transition Plan

FEA
Federal Enterprise Architecture

FFMIA
Federal Financial Management Improvement Act

FISMA
Federal Information Security Management Act

FM
Financial Management

FY
Fiscal Year

FYDP
Future Year Defense Program

GAO
Government Accountability Office

GIG
Global Information Grid

GOTS
Government Off-The-Shelf

HRM
Human Resources Management

ICD
Initial Capabilities Document

IPR
In-process review

IPT
Integrated Project Team

IR
Investment Review

IRB
Investment Review Board

IT
Information Technology

ITMA
Information Technology Management Application

JCIDS
Joint Capabilities Integration and Development System

JCS
Joint Chiefs of Staff

MAC I
Mission Assurance Category I

MAC II
Mission Assurance Category II

MAC III
Mission Assurance Category III

MACOM
Major Command

MAIS
Major Automated Information System

MDA
Milestone Decision Authority

MDAP
Major Defense Acquisition Program

MSSM
Material Supply and Service Management

NDAA FY05
Ronald W. Reagan National Defense Authorization Act of 2005 (PL 108-375)

NII
Networks and Information Integration

NSS
National Security System

OGC
Office of General Counsel

OMB
Office of Management and Budget

OSD
Office of the Secretary of Defense

OV
Operational View (DoDAF)

OV-1
DoDAF Operational View - High-Level Operational Concept Graphic

OV-2/5
DoDAF Operational View – Combined Operational Node Connectivity Description and Operational Activity Model

OV-3
DoDAF Operational View – Operational Information Exchange Matrix

OV-4
DoDAF Operational View - Organizational Relationships Chart

OV-5
DoDAF Operational View - Operational Activity Model

OV-6a
DoDAF Operational View - Operational Rules Model

OV-6c
DoDAF Operational View - Operational Event-Trace Description

OV-7
DoDAF Operational View - Logical Data Model

PA&E
Program Analysis and Evaluation

PCA
Pre-Certification Authority

PDA
Personal Digital Assistant

PEO
Program Executive Office(r)

PfM
Portfolio Management

PM
Program Manager

POM
Program Objective Memorandum

PPBE
Planning, Programming, Budgeting, and Execution

QDR
Quadrennial Defense Review

RDT&E
Research, Development, Test and Evaluation

SASA-BT
Special Assistant Secretary of the Army – Business Transformation

SECDEF
Secretary of Defense

SNAP-IT
Selective and Native Programming Data Collection System – Information Technology

SoS
System of Systems

SV

System View (DoDAF)

SV-1

DoDAF System View - Systems Interface Description

SV-4

DoDAF System View - Systems Functionality Description

SV-5

DoDAF System View – Operational Activity to Systems Function Traceability Matrix

SV-6

DoDAF System View - Systems Data Exchange Matrix

SV-8

DoDAF System View - Systems Evolution Description (Transition Plan)

TV

Technical View (DoDAF)

TV-1

DoDAF Technical View - Technical Standards Profile

USC

United States Code

USD (AT&L)

Under Secretary of Defense for Acquisition, Technology and Logistics

USD (C)

Under Secretary Defense (Comptroller)

USD (P&R)

Under Secretary of Defense for Personnel and Readiness

WMA

Warfighting Mission Area

WSLM

Weapon System Lifecycle Management

Section II
Terms

Acquisition

The acquiring by contract with appropriated funds of supplies or services (including construction) by and for the use of the Federal Government through purchase or lease, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated. Acquisition begins at the point when agency needs are established and includes the description of requirements to satisfy agency needs, solicitation and selection of sources, award of contracts, contract financing, contract performance, contract administration, and those technical and management functions directly related to the process of fulfilling agency needs by contract.

Acquisition Category

Categories established to facilitate decentralized decision-making and execution, and compliance with statutorily imposed requirements. The categories determine the level or review, decision authority and applicable procedures. Specific categories are defined below:

ACAT IA

Programs which are Major Automated Information Systems (MAIS) or programs designated by ASD (NII) to be ACAT IA. The Milestone Decision Authority is the DoD CIO. (3)

ACAT IAM

Is a sub-category of ACAT IA and is a program for which the Milestone Decision Authority (MDA) is the DoD Chief Information Officer (CIO). (3)

ACAT IAD

A MDA designated special interest program or a program that will require an eventual total expenditure for research, development, test and evaluation (RDT&E) of more than $365M. (3)

Application

A software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges.

Architecture

The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.

Army Business Enterprise Architecture (ABEA)

The framework of the business processes and organizations that support the Army’s warfighters.

Army Enterprise Architecture (AEA)

A disciplined, structured, comprehensive, and integrated methodology and framework that encompasses all Army information requirements, technical standards, and systems descriptions regardless of the information system’s use. The AEA transforms operational visions and associated required capabilities of the warfighters into a blueprint for an integrated and interoperable set of information systems that implements horizontal information technology insertion, cutting across the functional stove-pipes and Service boundaries. The AEA is the combined total of all the Army’s Operational, Technical, and System Architectures.

Army Information Technology Registry

The Army's enterprise data-base of record for information systems. The AITR is the source of the Army's data for input to the DoD Information Technology Registry. The AITR is one of the four submodules in the Army Portfolio Management Solution (APMS).

Army Standard System

A system that is standard across the Army.

Artifact

An Artifact is a graphical object that provides support information about the Process or the elements within the Process and it does not directly affect the flow of the Process.

Attribute

An Attribute is a property or characteristic that is common to some or all of the instances of a data Entity. For the Business Enterprise Architecture, an Attribute refers to the type of information DoD wants to retain about an Entity.

Automated Information System (AIS) Application

For DoD information assurance purposes, an AIS application is the product or deliverable of an acquisition program, such as those described in DODD 5000.1, "The Defense Acquisition System," May 12, 2003; Certified Current as of November 24, 2003. An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System, Defense Messaging System). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note that an AIS application is analogous to a "major application" as defined in OMB Circular A-130, "Management of Federal Information Resources, Transmittal 4," November 30, 2000; however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System.

Below Major Command

Systems which are not DoD-wide, Joint, Multi-Component, Component Standard Systems or Major Command Standard systems. Includes bridges (systems that interface between two or more other systems), uniques, and systems used at a single site.

Bridge

Systems that interface between two or more other systems.

Business Capability

The ability to execute a specific course of action and can be a single business enabler or a combination of business enablers – business process, people, tools or systems and information – that assists an organization in delivering value to its customers.

Business Enterprise Architecture (BEA)

The Business Enterprise Architecture is a blueprint to guide and constrain investments in DoD organization, operations, and systems as they relate to or impact business operations. It will provide the basis for planning, development, and implementation of business management systems that comply with Federal mandates and requirements, and will produce accurate, reliable, timely, and compliant information for DoD staff.

Business Mission Area (BMA) IT PfM

Business Mission Area IT Portfolio Management addresses all portfolio management activities in the DoD Business Mission Area.

Business Process

A Business Process is displayed within a Business Process Diagram (BPD). A Business Process contains one or more Processes.

Business Process Diagram (BPD)

A Business Process Diagram is the diagram specified by Business Process Modeling Notation. Business Process Diagram uses graphical elements and semantics to support elements defined in this specification.

Business System

A budgetary, strategic planning, accounting, finance, financial management, logistics, acquisition, human resources, real property/ personal property, mixed information system supporting financial and non-financial functions, or any information system that accepts or creates a transaction that results in a financial event or maintains the source data for a financial event for the DoD.

Business System Modernization

The acquisition or development of a new defense business system, or any significant modernization or enhancement of an existing defense business system other than necessary to maintain current services)

Capability

The highest level category of operational functions that provide the ability to accomplish a mission. “The ability to execute a specified course of action. It is defined by an operational user and expressed in broad operational terms in the format of an initial capabilities document or a DOTMLPF change recommendation. In the case of material proposals, the definition will progressively evolve to DOTMLPF performance attributes identified in the CDD and the CPD.” (CJCSI 6212.01D)

In the context of the AEA framework, a capability satisfies a requirement, specifically an IT requirement. For example, an Army headquarters element has the requirement to know the location of all friendly and enemy units in its area of operations; situational awareness is the capability that satisfies that requirement.

Capability Area

Collections of similar capabilities that are grouped at a high level in order to support decision-making, capability delegation, and analysis.

Capital Planning and Investment Management (CPIM)
The CPIM process is to develop C4/IT investment policy and strategic direction that informs Army leaders and directly impacts their POM decisions on all C4/IT expenditures across all functional domains. The CPIM process is collaborative among C4/IT stakeholders, with a focus on C4/IT across the Army (to include all functional domains) throughout the life cycle of IT expenditures and the management of IT assets.

Commercial-Off-The-Shelf (COTS)
COTS standards and customized software products or suites of products (e.g. featuring integration and/or bundling) used to perform typical office information processing functions and increase office productivity.

Community of Interest (COI)
A collection of people who exchange information using a common vocabulary in support of shared missions, business processes, and objectives. The community is made up of the users/operators who participate in the information exchange, the system builders who develop computer systems for these users, and the functional proponents who define requirements and acquire systems on behalf of the users.

Component
DoD component that is the originator of the funding source. DoD Components are defined to be the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Defense agencies, and the DoD field activities, and all other organizational and operational entities within the DoD.

Computer Network
The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities such as local or campus area networks, or long-haul data transport capabilities such as operational, metropolitan, or wide area and backbone networks.

Core System
An existing system, a system in development, or a system beginning the acquisition process that is/will become the Department’s solution for a given capability(ies), as designated by the CBMA.
COTS Office Automation Software Products/Suites COTS software products or suites of products used to perform typical office information processing functions and increase office productivity.

Criteria
Standards, measures, and/or expectations used in making an evaluation and/or verification.

Data

Data is a representation of an individual fact, concept, or instruction in a manner suitable for communication, interpretation, or processing by humans or by automatic means.

Data Element

A Data Element represents information required to support a process. Data elements are defined in the Integrated Dictionary (AV-2) and referenced in the Logical Data Model (OV-7) and the Process Model (OV-6c) and other diagrams. In the BEA, the same information is always conveyed through the same agreed-upon named data element regardless of which process or activity sends or receives the information.

Data Management Initiatives

These include the policy, procedures and mechanism that ensure visibility, accessibility, semantic interoperability and metadata tagging of data.

Data Model

A Data Model is a graphical and textual representation of analysis that identifies the data needed by an organization to achieve its mission, functions, goals, objectives, and strategies and to manage and rate the organization. A data model identifies the entities, attributes, and relationships (or associations) with other data, and provides the conceptual view of the data and the relationships among data.

Data Object

A Data Object represents a set of data elements that can be associated with a sequence flow or a process step (activity) in a Process Model.

Data Store (or Data Warehouse)

A data store or data warehouse is a static database that contains historical data, and is strictly used for data analysis (e.g. trends).

Domain

An area of common operational and functional requirements. A subset of Mission Areas that represent a common collection of related, or highly dependent, information capabilities and services. The Domain manages portfolios of information capabilities and services.

Enclave

A collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, as well as common applications such as office automation and electronic mail.

End-to-End Process

The End-to-End Process is the scope of the business area under examination; characterized by an essential business event, result, and process that broadly connect them (for example, Order to Cash). An End-to-End Process typically includes a number of component business processes to support it (for example, Order to Cash usually includes Customer Acquisition, Order Management, Order Fulfillment, and Account Receivable) and usually includes processes that span component processes (for example, Order Returns).

Enterprise

Refers to the Department of Defense, including all of its organizational entities.

Enterprise Architecture

A DoD-wide architecture that depicts warfighting and business Domains.

The explicit description of the current and desired relationships among business and management processes and IT. An enterprise architecture describes the “target” situation that the agency wishes to create and maintain by managing its IT portfolio.

Enterprise Data Model

The Enterprise Data Model provides an integrated model of the data pertinent to the DoD business Domains. It aims to provide a record of accurate and meaningful business data definitions, and identify valid, consistent business data structures that contain information to run and manage the business. The purposes of the BEA Enterprise Data Model are to:

- provide a single development base and promote the integration of existing applications where appropriate
- serve as a data reference architecture to support the sharing of data across the DoD Business Domains
- enable effective management of data resources by providing a single set of consistent data definitions, and,
- support the creation and maintenance of BMA enterprise-wide data

The Enterprise Data Model encompasses two distinct views, a conceptual view that reflects a high-level overview, and a logical view that provides additional details of the data pertinent to DoD business Domains.

Enterprise Information Environment (EIE)

The common, integrated information computing and communications environment of the GIG. The EIE is composed of GIG assets that operate as, provide transport for and/or assure local area networks, campus area networks, tactical operational and strategic networks, metropolitan area networks, and wide area networks. The EIE includes computing infrastructure for the automatic acquisition, storage, manipulation, management, control, and display of data or information, with a primary emphasis on DoD enterprise hardware, software operating systems, and hardware / software support that enable the GIG enterprise. The EIE also includes a common set of enterprise services, called Core Enterprise Services, which provide awareness of, access to, and delivery of information on the GIG.

Enterprise Portals

A web site or service that offers a broad array of resources and services, such as e-mail, forums, search engines, on-line self-service applications, security, directory, profiling, taxonomy, application integration.

Enterprise Process
Enterprise processes are those end-to-end groupings of integrated and interrelated functions across Domain and Mission Areas that provide mission-critical capabilities to the warfighter, and form the basis for the enterprise architecture.

Enterprise Process Owners
Key decision makers on Army Enterprise process issues; interface with the Mission Area and Domain Leads to conduct Portfolio Management of process enablers; approve end-to-end process scenarios to facilitate design and implementation of process capabilities; and champion the use of Enterprise Solutions as process enablers.

Entity
A data Entity is defined as a representation of a set of real or abstract things (people, objects, places, events, ideas, or a combination of things, etc.) that are recognized as the same type, because they share the same characteristics and can participate in the same relationships. For BEA purposes, a data entity is a kind of object that the DoD uses to retain information.

Extract
Access data from a specified source database and extracts a desired subset of data.

Family of Systems
A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities dependent on the situation.

Financial and “mixed” systems
The term "mixed system" means an information system that supports both financial and non-financial functions of the Federal government or components thereof. Refer to Circular A-127 or A-130 requires that executive agencies develop and maintain an agency wide inventory of financial management systems and ensure that appropriate assessments of these systems are conducted. These Circulars applies to financial management systems, which includes financial and mixed systems.

Focus Area
Definition of the concentration point for portfolio evaluation used to slice and dice the portfolio perspective (e.g. ERP, gaps, redundancies).

Global Information Grid (GIG)
The globally connected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

Governance

The process through which organizations make strategic decisions, determine whom they involve and demonstrate accountability for the results of their actions. The process of governance relies on a system or framework – to include Federal statutes; DoD and Army directives, policies or guidelines; steering committees or groups; and performance measures – to define how the process is supposed to function in a particular setting. Cultural traditions, accepted practices, and codes of conduct are also instrumental in influencing the governance process. Ideally, the governance process achieves agreement between differing interests to reach a broad consensus on what is in the best interest of the enterprise.

Information

Any communication or representation of knowledge such as facts, data, or opinion in any medium or form, including textual, numerical, graphic, cartographic, or narrative.

Information Assurance (IA)

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Life Cycle

The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

Information Management

The planning, budgeting, manipulating, and controlling of information throughout its life cycle.

Information Resources

Information and related resources, such as personnel, equipment, funds, and information technology.

Information Resources Management

The process of managing information resources to accomplish Agency missions and to improve Agency performance, including through the reduction of information collection burdens on the public.

Information System

Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and that includes computer software, firmware, and hardware. Included are computers, word processing systems, networks, or other electronic information handling systems and associated equipment.

Information Technology (IT)

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the DoD Component. For the purposes of the preceding sentence, equipment is used by a DoD Component if the equipment is used by the DoD component directly or is used by a contractor under a contract with the DoD component that (1) requires that use of such equipment, or (2) requires the use, to a significant extent of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related sources. For purposes of the preceding sentence, equipment is used by an executive agency (DoD) or if the equipment is used directly by the DoD or is used by a contractor under a contract with the executive agency (DoD) which requires the use of such equipment or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Information Technology (IT) Investment
The development and sustainment resources needed in support of IT or IT-related initiatives (e.g., applications, programs, projects, services, studies, systems, telecommunications, tools and system support service contracts). These resources include, but are not limited to: research, development, test and evaluation (RDT&E) appropriations; procurement appropriations; military personnel (MILPERS) appropriations; operations and maintenance (O&M) appropriations; and Defense Working Capital Fund (DWCF).

Information Technology (IT) Labor Skill
Any human resource used to perform information technology requirements.

Information Technology (IT) Portfolio
A grouping of IT investments by capability to accomplish a specific functional goal, objective, or mission outcome.

Information Technology (IT) System
Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Any Acquisition Category (ACAT) system that meets these criteria, anything categorized as a National Security System (NSS) or a Mission Assurance Category (MAC) level is, by definition, considered to be an IT system. Other types of IT systems include:

- DoD-wide, Joint systems
- Federal System used by DoD or supported by DoD
- DoD System used as a Federal System
- Multi- System
- Standard System
- Major Command Standard System (Echelon 2 or equivalent for Navy and Marine Corps)
- Below Major Command System (below Echelon 2 or equivalent for Navy and Marine Corps) (e.g., bridges, unique used at a single site)
- Data Stores/Data Warehouses
- Enclaves
- Portals (Enterprise)

- Automated Information System (AIS) Application

Infrastructure

The term is used with different contextual meanings. It most generally relates to and has a hardware orientation, but it is frequently more comprehensive and includes software and communications. Collectively, the structure must meet the performance requirements of and capacity for data and application requirements. It includes processors, operating systems, service software, and standards profiles that include network diagrams showing communication links with bandwidth, processor locations, and capacities to include hardware builds versus schedule and costs.

Initiative

Initiatives are IT systems, programs, projects, organizations, activities or family of systems.

Integration

The process of making or completing by adding or fitting together into an agreed framework (architecture) the information requirements, data, applications, hardware, and systems software required to support the Army in peace, transition, and conflict.

Interim System

An existing system or system in development, as designated by the CBMA, that supports the Department for a given capability during a limited period of time until the core system is deployed.

Internal Script

A series of commands, launched by a single action, performed by the client.

Interoperability

The ability of two or more systems, units, forces, or physical components to exchange and use information. The conditions achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily.

IT Capital Planning and Investment Control (CPIC)

An end-to-end integrative process that frames and manages the life cycle of an IT investment. Its purpose is to maximize the value and assess and manage the risks of the IT acquisitions of the Army. The process includes the selection, management, and evaluation of IT investments.

IT Portfolio

A grouping of IT investments by capability to accomplish a specific functional goal, objective, or mission outcome.

IT Investment Portfolio

A collection of IT investments that represents the best balance of costs, benefits, and risks and is designed to improve the overall organizational performance and maximize mission performance.

IT that is not part of the Global Information Grid(GIG)
Generally, stand-alone, self-contained, or embedded IT that is not and shall not be connected to the enterprise network.

Joint
Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate. (Joint Pub 1-02)

Lean / Six Sigma
An improvement methodology and mindset that integrates Lean concepts (increase speed, reduce waste) and Six Sigma concepts (reduce variation, improve quality) that enable organizational transformation at all levels.

Legacy System
An existing system that is designated for closure when the capability is absorbed by an interim or core system, or an existing system without any designation yet made.

Major Automated Information System or Project (MAIS)
An AIS acquisition program that is (1) designated by ASD(C3I) as a MAIS, or (2) estimated to require program costs in any single year in excess of 30 million in fiscal year (FY) 1996 constant dollars, total program costs in excess of 120 million in FY 1996 constant dollars, or total life-cycle costs in excess of 360 million in FY 1996 constant dollars. MAISs do not include highly sensitive classified programs (as determined by the Secretary of Defense). For the purpose of determining whether an AIS is a MAIS, the following shall be aggregated and considered a single AIS: (1) the separate AISs that constitute a multi-element program; (2) the separate AISs that make up an evolutionary or incrementally developed program; or (3) the separate AISs that make up an a multi-component AIS program.

Major Command Standard
A system that is standard across a Major Command.

Management Decision Evaluation Package (MDEP)
An 8-year package of dollars and manpower to support a given program or function. The BIP is the first 3 budget and execution years of the MDEP and the PDIP is the 5 program years following.

Metrics
The elements of a measurement system consisting of key performance indicators, measures, and measurement methodologies.

Mission Area (MA)
A defined area of responsibility with functions and processes that contribute to mission accomplishment.

Mission Assurance Category

Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories.

Mission Assurance Category I (MAC I)
Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures. (6)

Mission Assurance Category II (MAC II)
Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure assurance. (6)

Mission Assurance Category III (MAC III)
Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Mission Assurance Category III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices. (6)

Mission Critical Information System
A system that meets the definitions of "information system" and "national security system" the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (Note: The designation of mission critical shall be made by a DoD Component Head, a Combatant Commander, or their designee. A financial management Information Technology (IT) system shall be considered a mission-critical IT system as defined by the Under Secretary of Defense (Comptroller).) A "Mission-Critical Information Technology System" has the same meaning as a "Mission-Critical Information System"

Mission Essential Information System
A system that meets the definition of "information system" that the acquiring DoD Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (Note: The designation of mission essential shall be made by a DoD Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-essential IT system as defined by the Under Secretary of Defense

(Comptroller) a "Mission-Essential Information Technology System" has the same meaning as a "Mission-Essential Information System.

Mission Support Information System
System that is not defined as mission critical or mission essential.

Model
A conceptual framework of standards for communication in the network across different equipment and applications by different vendors.

Modernization
All costs, of any type of funding, incurred to design, develop, implement/deploy and/or functionally enhance/technically upgrade an information technology system. These costs include, but are not limited to, personnel, equipment, software, supplies, and contracted services from private sector providers, space occupancy, and intra-agency services from within the agency and inter-agency services from other Federal agencies. Does not include sustainment costs. Sources, OMB A-11, A-130.

Module
A distinct element of a “system” that CANNOT stand alone outside of its system’s environment.

National Security Systems (NSS)
Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but excluding any system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Net-Centricity
A global, web-enabled environment which ensures user-focused information sharing, information fusion, sense making, and decision-making across the Battlespace; and makes it possible to move beyond traditional communities of interest, such as command and control or intelligence, to full cross-functional information exchange across the Battlespace.

Network
Communications medium and all components attached to that medium whose function is the transfer of information.

Open Database Connectivity Object (ODBC)
An open standard application programming interface (API) for accessing a database allowing access to files in a number of different databases (i.e. Access, dBase, DB2, Excel, Text, etc.).

Operational Architecture

Descriptions of the tasks, operational elements, and information flows required to accomplish or support a function.

Opportunity Set
Potential IT solutions to business capability requirements based on a capability or groups of capabilities which produce the best solution for achieving the identified business capability requirements.

Performance Measure
A quantitative or qualitative characterization of performance.

Performance Measurement
A process of accessing progress toward achieving predetermined goals, including information on the efficiency with which resources are transformed into goods and services (outputs), the quality of those outputs (how well they are delivered to clients and the extent they are satisfied), and outcomes (the results of a program activity compared to its specific contributions to program objectives.

Peripheral Equipment
Any of a variety of devices that are attached to a computer (i.e. auxiliary storage units, storage units, disk drives, drum drives, magnetic storage devices, optical storage devices, recorders, tape, monitors, keyboards, etc.).

Personal Digital Assistant (PDA)
Mobile computing devices such as laptops, handhelds, and personal digital assistants operating in either wired or wireless mode, or other information technologies as may be developed.

Planning, Programming, Budgeting, and Execution (PPBE) process
The process for justifying, acquiring, allocating, and tracking resources in support of Army missions.

Portal
Portals provide a single web “location” from which many services and communications systems are accessed. May also be the establishment of a single secure web access point from which applications and information may be distributed. To enable enterprise portal services there must be: Web services, a global directory service, and PKI.

Portfolio
The group of capabilities, resources, management, and related investments that are required to accomplish a mission-related or administrative outcome. A portfolio includes outcome performance measures (mission, functional or administrative measures) and an expected return on investment. For purposes of this definition, “resources” consists of people, money, facilities, weapons, information technology, other equipment, logistics support, services and information, and “management” consists of strategic planning, capital planning, governance, process improvements, performance metrics/measures, requirements generation, acquisition/development and operations.

Portfolio Management

The management of selected groupings of IT investments using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability.

Process

An ordered sequence of events involving people, materials, energy, and equipment that is designed to achieve a defined business outcome. A process is depicted as a network of flow objects, which are a set of activities and the controls that sequence them. A group of logically related decisions and activities required to manage the resources of the Army. A business process is a specific ordering of work activities across time and place, with a beginning, an end, and clearly defined inputs and outputs that deliver value to customers.

Process owners

HQDA functional proponents, MACOMs, and others who have responsibility for any mission-related or administrative work process.

Redundant

a. Exceeding what is necessary or normal (superfluous); characterized by or containing an excess, specifically using more words than necessary; characterized by similarity or repetition

b. Serving as a duplicate for preventing failure of an entire system (as a spacecraft) upon failure of a single component

c. Unnecessary duplication of capabilities, investments, processes, systems, programs and other entities identified by gap and overlap analysis.

Reference Business Process Model (RBPM)

The Reference Business Process Model identifies taxonomy of DoD business macro processes, sub-processes that comprise them, and related process threads for Business Management Modernization Program.

Relationship

A Relationship determines associations between data entities, categorized as identifying/non-identifying, specific/non-specific or categorizing, and identified in terms of cardinality and optionality. Relationships express and enforce business rules that govern the behavior and dependence of data.

Report

An organized view that sort a collection of data, prepared for viewing or printing from multiple records.

Software

A set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system (for example, compiler, library routines, manuals, circuit diagrams); usually contrasted with hardware.

Stove-pipe

An entity, i.e., a system, organization, process, etc., whose design does not support effective information sharing or leveraging of capabilities with other, related entities.

Stovepipe Application
A stand-alone program. An application that does not integrate with or share data or resources with other applications.

Stovepipe System
Non-interoperable domain application with services developed and deployed using disparate architectural frameworks. Interoperability was never designed into the system.

SubDomain
A subset of Domains that represent a common collection of related, or highly dependent, information capabilities and services. The SubDomain manages portfolios of information capabilities and services.

Sub-Portfolio
The allocation of business systems within a defined boundary. The boundary for a sub-portfolio may be defined by a specific service/agency, process owner, executive agent, etc.

Sub-System
A distinct element of a “system” that CAN stand alone outside of its system’s environment.

System
A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. An organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions (see JCS 1–02). Within the context of the Army Enterprise Architecture, systems are people, machines and methods organized to accomplish a set of specific functions; provide a capability or satisfy a stated need or objective; or produce, use, transform, or exchange information. For the purpose of reporting to the Army Information Technology Registry, the terms “application” and “system” are used synonymously—a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information (that is, the application of IT).

System Data Exchange
A Systems Data Exchange is the movement of data between the entity, the process, and the data store. Data flow portrays the interface between components of the Data Flow Diagram (DFD). The flow of data in a DFD is named to reflect the nature of the data used (these names should also be unique within a specific DFD. An arrow represents data flow and the arrow annotates the direction of data flow.

System Entity
A logical grouping of system functions that have a high affinity for each other in terms of the data they manage and which address the processing requirements of a definable business

application. A system entity logically organizes a set of system functions into a cohesive group of common functionality.

System Function

Each component of a system entity that manipulates inputs to produce desired outputs in accordance with established business rules is referred to as a system function. System functions represent processes performed by people, machines, or a combination of both and may be depicted on the SV-4 diagram as a circle (those which are internal to the process described by the diagram title) or a rectangle (those which are external to the process described in the diagram title).The process is the manipulation or work that transforms data, performing computations, making decisions (logic flow), or directing data flows based on business rules. In other words, a process receives input and generates some output. Process names (simple verbs and data flow names, such as “Submit Payment” or “Get Invoice”) usually describe the transformation, which can be performed by people or machines. Processes can be drawn as circles or a segmented rectangle on a Date Flow Diagram, and include a process name and process number.

System of Systems (SoS)

A set or arrangement of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole. An example of a SoS system could be interdependent information systems. While individual systems within the SoS may be developed to satisfy the peculiar needs of a given user group (like a specific Service or agency), the information they share is so important that the loss of a single system may deprive other systems of the data needed to achieve even minimal capabilities.

The Army Plan

This plan is a 16-year strategic planning horizon that includes the 6-year span of the program (POM) years plus an additional 10 years. TAP presents comprehensive and cohesive strategic, midterm planning and programming guidance that addresses the Army’s enduring core competencies over this time period.

Transition Planning

The activities associated with developing the plan and framework for moving from the “As Is” to the “To Be” using strategic plans, Business Capabilities, and architecture information. It incorporates investment management decisions made during the Portfolio Management, PPBE, DAS, and JCIDS processes. It includes the identification of gaps between the “As Is” and the “To Be.”

Unique

Systems used at more than one site below Major Command level.

Warfighter

A common soldier, sailor, airman, or marine by trade, from all Services who joins in a coordinated operation to meet a common enemy, a common challenge, or a common goal.

Warfighting Mission Area

Warfighting Mission Area (WMA) assets (IT and NSS) enhance joint warfighting while supporting actions to create a joint, network-centric distributed force, capable of full spectrum dominance through decision and information superiority. WMA assets ensure COCOMs can win the War on Terrorism; fight as a Joint Force; and transform "in stride" – fielding new capabilities and adopting new operational concepts while actively taking the fight to the enemy. WMA assets that are knowledge empowered, networked, interoperable, expeditionary, adaptable/tailorable, enduring, precise, fast, resilient, agile and lethal. (See National Military Strategy, 2004 and the Capstone for Joint Operations, Aug 2005)